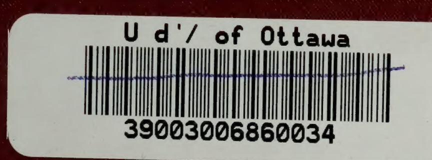

U d'/ of Ottawa
39003006860034

See Corrections
Bulletin Nov-Dec 19

THÉORIE DES NOMBRES

PARIS. — IMPRIMERIE GAUTHIER-VILLARS ET Cie,
66178 Quai des Grands-Augustins, 55.

THÉORIE DES NOMBRES

PAR

M. KRAÏTCHIK,

INGÉNIEUR A LA SOCIÉTÉ FINANCIÈRE DES TRANSPORTS
ET D'ENTREPRISES INDUSTRIELLES,
DIRECTEUR A L'INSTITUT DES HAUTES ÉTUDES DE BELGIQUE.

AVEC UNE PRÉFACE

de M. d'OCAGNE,

Membre de l'Institut.



PARIS

GAUTHIER-VILLARS ET CIE, ÉDITEURS

LIBRAIRES DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE

55, Quai des Grands-Augustins, 55

1922



PRÉFACE

J'ai eu, à diverses reprises, l'occasion de faire remarquer que, contrairement à un préjugé assez répandu, il n'est pas ordinaire de trouver réunis chez une même personne un talent distingué de mathématicien et une aptitude particulière pour le calcul numérique; il s'agit, en réalité, là de deux dons parfaitement distincts, de même que ceux de la composition et de l'exécution musicales; encore un compositeur de musique sera-t-il bien plus généralement bon exécutant qu'un mathématicien habile calculateur; tels illustres analystes, ayant puissamment contribué au progrès de nos connaissances dans les parties les plus élevées de la théorie pure, n'ont jamais cessé de se montrer, dans le maniement des chiffres, d'une véritable maladresse. Ce n'est donc pas donner de l'auteur de cet Ouvrage une caractéristique banale que de dire qu'il est à la fois bon mathématicien et très remarquable calculateur; il peut, suivant la locution de Jacobi, chère à Hermite, être regardé comme un *vir arithmeticus;* il se trouvait donc voué, en quelque sorte, par prédestination, à poursuivre les études d'où est sortie cette *Théorie des nombres* qu'il m'a fait l'honneur de me demander de présenter au public.

J'ai accepté d'autant plus volontiers de le faire (bien que n'ayant point de compétence spéciale en la matière), que M. Kraïtchik, qui s'est fait connaître comme un ingénieur distingué, en même temps qu'il poussait fort loin

ses études mathématiques, s'est aussi classé parmi les adeptes les plus fervents de la nomographie dont il a publié nombre de très importantes applications, particulièrement aux calculs financiers. Cela atteste la souplesse de son esprit capable de se plier à la fois à la rigide discipline de la théorie du nombre pur et à la multiple variété des procédés destinés à réduire à son maximum de simplicité l'exécution des calculs approchés, seulement requis par les besoins de la pratique courante. Les habitudes d'esprit qu'il a prises en se familiarisant avec ces procédés ne l'ont d'ailleurs peut-être pas desservi au cours de ses études de pure théorie des nombres. On verra, en effet, quel parti il a su tirer de certains procédés graphiques — voire mécaniques — dans ses recherches relatives aux propriétés des nombres entiers.

La théorie des nombres occupe une place à part dans le domaine des mathématiques, et son développement n'a pas été absolument concomitant de celui des autres parties de ce domaine, ses plus notables progrès s'étant produits, en quelque sorte, par brusques à-coups.

L'aurore de cette discipline spéciale est dominée par deux grands noms, ceux de Fermat et d'Euler.

La participation de Fermat (1601-1665) à l'éclosion de cette science ne laisse pas d'être entourée d'une sorte de mystère; ce profond mathématicien s'est borné à formuler les énoncés des théorèmes qu'il avait découverts en faisant de leur démonstration, proposée aux autres chercheurs, l'objet d'une sorte de défi. Il n'a d'ailleurs jamais fait connaître lui-même la voie par laquelle il les a obtenus, se bornant à affirmer que s'il la divulguait, on serait étonné de sa simplicité.

Émanant d'un homme tel que lui, une telle déclaration ne doit pas être regardée comme faite à la légère, et cela incite d'autant plus à déplorer qu'il n'ait jamais révélé le secret de sa méthode, vu les efforts qui ont été dépensés

depuis lors par nombre de chercheurs, dont quelques-uns des plus éminents, pour venir à bout des questions ardues qu'il a offertes à leur sagacité. Ces efforts ont, au reste, été couronnés de succès dans un grand nombre de cas et n'ont abouti jusqu'ici à infirmer qu'une seule proposition avancée par Fermat, celle-ci, au reste, sous forme dubitative (voir plus loin p. 3 et 21). De celles qu'il a formulées sans réserve, aucune, si l'on n'est pas encore parvenu à l'établir, n'a en tout cas été trouvée en défaut.

Parmi les vainqueurs de cette sorte de tournoi arithmétique, une place à part revient à Euler (1707-1783) dont le génie, universel en mathématiques, s'est attaché en particulier à ce sujet difficile.

L'objet de cette étude étant principalement la recherche des propriétés des nombres entiers, donc d'une suite essentiellement discontinue, échappait *a priori* aux méthodes de l'analyse infinitésimale; d'où la nécessité de créer des modes d'investigation entièrement différents qui lui fussent spécialement applicables; telle a été, en ce domaine, l'œuvre propre d'Euler.

Depuis lors, de nouveaux horizons ont été ouverts sur cette science captivante par les travaux de plusieurs grands mathématiciens, parmi lesquels je me bornerai à citer Lagrange, Legendre, Gauss, Lejeune-Dirichlet, Hermite.

Mais, bien que se rattachant encore étroitement par leur essence à l'arithmétique supérieure, ces travaux débordent le cadre primitif où les premiers pionniers de cette branche spéciale avaient borné l'objet de leurs explorations. C'est la théorie arithmétique des formes quadratiques à deux variables que cette nouvelle pléiade de chercheurs a eu surtout en vue.

Rappelons d'un mot de quelle extraordinaire fécondité s'est montrée l'idée, conçue par le génie d'Hermite, de l'introduction, en ce domaine, de variables continues,

fécondité encore attestée dernièrement par les élégantes recherches poursuivies par Georges Humbert, pendant les dernières années de sa carrière trop tôt terminée.

Pour en revenir à la théorie des nombres proprement dite, il convient de noter qu'en dépit de sa prodigieuse ingéniosité, Euler n'a pu absolument affranchir ses procédés d'investigation d'une sorte de tâtonnement ou, plus exactement, de recours à la méthode expérimentale consistant en des séries d'essais numériques propres à réaliser un véritable *criblage*. Hermite aimait à souligner ce caractère quasiment expérimental de certaines recherches d'arithmétique pure.

Il va sans dire que ce mode opératoire, véritablement fondé sur l'expérience, ne vise que la résolution de certains problèmes, non la démonstration des théorèmes qui exige, comme dans les autres parties des mathématiques, toute la rigueur des raisonnements purement logiques.

Mais, quand il s'agit de résoudre des problèmes, il convient de noter que, même dans les cas où l'on peut donner une solution directe, l'emploi du procédé par tâtonnement, tout aussi sûr, l'emporte généralement en simplicité. (Comparer à cet égard les n°s 24 et 25 du Chapitre IV, p. 83 et 85.)

Le tâtonnement devant, d'après cela, être regardé comme inévitable en ce genre de recherche, la question qui se posait consistait à le perfectionner. L'introduction par Euler des diviseurs linéaires de formes quadratiques, dont l'usage fut étendu par Gauss, permit déjà de réaliser, à cet égard, un sensible progrès.

Il y avait néanmoins plus encore à faire : il s'agissait d'imaginer des procédés opératoires aussi sûrs, faciles et rapides que possible, permettant d'effectuer les criblages dont il vient d'être question sur des ensembles de nombres assez considérables pour décourager toutes les tentatives poursuivies par les voies ordinaires. C'est ici qu'inter-

vient l'intéressante contribution due, en ces matières, à M. Kraïtchik lui-même.

Alors que les procédés de criblage anciens ne pouvaient guère s'appliquer pratiquement à plus d'une trentaine ou une quarantaine de valeurs possibles, celui de M. Kraïtchik permet, sans plus de dépense d'effort ni de temps, d'étendre l'opération à des ensembles comprenant plusieurs millions et même plusieurs dizaines de millions de nombres, sans que, grâce à l'emploi d'un dispositif graphique approprié, il soit nécessaire d'écrire ces nombres.

M. Kraïtchik est même allé plus loin; il a imaginé un projet de machine (voir p. 43) qui permettrait l'application purement automatique du procédé et son extension à des ensembles pouvant comporter des milliards de valeurs à étudier.

J'ai tenu à insister sur ce qui précède pour mieux mettre en lumière la part qui, dans le travail qu'on va lire, revient plus personnellement à l'auteur; mais, en fait, dans la façon de présenter les parties plus classiques de son sujet et d'établir les démonstrations, il fait encore montre d'une incontestable originalité.

Le présent Volume, borné à ce qui constitue les éléments proprement dits de la théorie des nombres, peut être considéré comme une sorte d'introduction à cette théorie. Il est dans les intentions de M. Kraïtchik de poursuivre, dans des Volumes ultérieurs, l'exposé des développements théoriques qui s'y rattachent.

Tel qu'il est, ce premier Volume, grâce en partie à l'abondance des tables numériques auxiliaires qu'il renferme, me semble appelé à rendre déjà de grands services à tous ceux qu'attirent les recherches variées auxquelles les nombres peuvent donner naissance.

M. d'Ocagne,

de l'Académie des Sciences.

THÉORIE DES NOMBRES

CHAPITRE I.

GÉNÉRALITÉS.

---

1. Un nombre N est dit *premier* s'il n'est divisible par aucun autre nombre, excepté les nombres 1 et N. Tels sont les nombres :

$$2.3.5.7.11\ldots 2^{31}-1\ldots 2^{61}-1\ldots 5.2^{75}+1\ldots 2^{89}-1\ldots 2^{107}-1\ldots 2^{127}-1\ldots.$$

Tout nombre qui n'est pas premier est composé et est divisible par quelques autres nombres. Tels sont :

$$4.6.8.9.10.12.14.15\ldots 2^{128}+1\ldots 2^{256}+1\ldots.$$

Le plus petit diviseur d'un nombre composé est un nombre premier ; car si N n'est pas un nombre premier, il est divisible par N_1, ce nombre étant compris entre 1 et N. Si N_1 n'est pas premier, il est divisible à son tour par $N_2 > 1$ et N_2 sera aussi diviseur de N.

En effet, si N est divisible par N_1, on aura $N = N_1 q$. Si N_1 est divisible par N_2, on aura de même $N_1 = N_2 q$, donc $N = N_2 qq'$.

Si N_2 n'est pas premier, il est à son tour divisible par $N_3 > 1$ et ce nombre N_3 sera aussi diviseur de N, etc. ; le plus petit diviseur sera donc nécessairement un nombre premier.

2. *La suite des nombres premiers est illimitée.*

Nous allons démontrer qu'étant donné un nombre premier N, aussi grand qu'on le veut, il existe toujours un nombre premier plus grand que N.

Considérons à cet effet le nombre P(N) formé en multipliant entre eux tous les nombres premiers depuis 2 jusque N :

$$P(N) = 2.3.5.7.11\ldots N,$$

et considérons le nombre $P(N)+1$ qui n'est divisible ni par 2, ni par 3, ni par 5,..., ni par aucun nombre premier inférieur à N. Si le nombre $P(N)+1$ est premier, le théorème est démontré. Dans le cas contraire, son plus petit diviseur est premier, et ce plus petit diviseur sera supérieur à N. Il existe donc, même dans ce cas, un nombre premier supérieur à N. Dans les deux cas, le nombre N n'est pas le *dernier* nombre premier, et il n'en existe pas.

3. Toutefois, les nombres premiers deviennent de plus en plus rares dans la suite des nombres entiers. C'est ainsi qu'on compte 168 nombres premiers de 1 à 1000 (le nombre 1 n'est pas compris dans ces 168 nombres). On n'en trouve plus que 135 de 1000 à 2000, 77 entre 199000 et 200000, 71 entre 10000000 et 10001000, 54 entre 10^8 et 10^8+1000, 49 entre 10^9 et 10^9+1000, etc.

Nous donnerons dans le deuxième Volume plus de détails à ce sujet. Pour le moment, bornons-nous à dire qu'on possède actuellement des Tables des nombres premiers jusqu'à 10^7 (plus exactement jusqu'à 10017000).

Ce sont les Tables de Lehmer (Factor Table). Elles donnent le plus petit diviseur des nombres composés non divisibles par 2, 3, 5 et 7.

4. Depuis longtemps on s'est occupé de la question de savoir s'il existe une formule qui n'exprime que des nombres premiers, tous les nombres premiers ou certains d'entre eux. Euler a démontré qu'il n'existe aucun polynome algébrique de ce genre. Soit

$$F(x) = a + bx + cx^2 + dx^3 + \dots$$

un polynome qui pour $x = n$ donne le nombre premier N, de sorte que

$$N = a + bn + cn^2 + dn^3 + \dots.$$

Si l'on fait

$$x = n + kN,$$

on obtiendra pour $F(x)$ un nombre divisible par N, donc non premier.

Fermat croyait avoir la solution de ce problème avec la formule

$$F_n = 2^{2^n} + 1$$

qui donne :

Pour $n = 0$	$F_n =$	3
» 1		5
» 2		17
» 3		257
» 4		65 537

Toutes ces valeurs de F_n sont bien premières. Il croyait donc pouvoir affirmer que tous les nombres de la forme précitée sont premiers. Or, Euler a démontré que pour $n = 5$ on trouve

$$F_5 = 641 \times 6700417.$$

Depuis, on a trouvé bien d'autres résultats infirmant l'assertion de Fermat. Nous donnons la liste de tous les résultats connus au paragraphe 6, Chapitre II.

Toutefois, on trouve des polynomes qui donnent beaucoup de nombres premiers. Telles sont les formules

$$x^2 + x + 17, \quad 2x^2 + 29, \quad x^2 + x + 41$$

qui donnent 17, 29 et 41 nombres premiers pour les 17, 29, 41 valeurs croissantes de x en commençant par $x = 0$.

5. Deux nombres sont premiers entre eux s'ils n'ont pas de facteurs communs. Tels sont les nombres 14 et 15, $2^n - 1$ et $2^n + 1$.

Si N est un nombre premier, il sera premier avec tout nombre qu'il ne divise pas, et en particulier avec tous les nombres qui lui sont inférieurs.

On appelle *plus grand diviseur de deux nombres*, le plus grand nombre qui divise chacun des nombres donnés.

Le plus grand diviseur de deux nombres A et B sera désigné par la notation D(A, B).

Tout diviseur du plus grand diviseur de deux nombres est aussi un diviseur commun de ces nombres et sera désigné par la notation d(A, B).

Le plus grand commun diviseur de nombres premiers entre eux est 1.

Le plus grand commun diviseur de deux nombres dont le plus

petit divise l'autre est le plus petit de ces nombres :

$$D(A, KA) = A.$$

Le plus grand commun diviseur de deux nombres quelconques est égal au plus grand commun diviseur du plus petit nombre et, du reste, de la division du plus grand par le plus petit.

Ainsi, si $B = Aq + R$, on aura

$$D(A, B) = D(A, R).$$

Il en résulte que l'algorithme du plus grand commun diviseur est le même que celui des fractions continues.

6. *Si* A *et* B *sont premiers avec* C, *le produit* AB *est aussi premier avec* C.

En effet, cherchons le plus grand commun diviseur de A et C par une série d'égalités :

$$A = cq_1 + R_1, \qquad C = R_1 q_2 + R_2, \qquad \ldots, \qquad R_{n-2} = R_{n-1} Q_n + R_n,$$

on aboutira à $R_n = 1$, car par hypothèse $D(AC) = 1$.

Si l'on multiplie ces égalités par B, il vient

$$AB = CBq_1 + R_1 B,$$
$$CB = R_1 Bq_2 + R_2 B, \qquad \ldots, \qquad R_{n-2} B = R_{n-1} Bq_n + R_n B.$$

Ces dernières égalités expriment successivement :

$$D(AB, C) = D(C, R_1 B) = D(C, R_2 B) = \ldots = D(C, R_n B) = D(CB) = 1.$$

Corollaires :

1° $$D(AB, AC) = A.D(B, C);$$

2° Si C est premier avec A et divise le produit AB, C divise B;

3° Si A et B sont premiers entre eux et que chacun divise C, le produit AB divise aussi C.

En effet, soit $C = AQ$. Puisque B divise C ou AQ tout en étant premier avec A, B divise Q. Soit $Q = BQ_1$, donc $C = ABQ_1$ et par conséquent le produit AB divise C.

7. Si l'on décompose le nombre N en ses facteurs $N = a^m b^n c^p \ldots$, on voit que N est premier avec tout nombre ne contenant aucun

des facteurs a, b ou c. Par contre, N est divisible par tout nombre $N' = a^{m'} b^{n'} c^{p'} \ldots$ qui ne contient que les facteurs a, b, c avec des exposants m', n', p', ... respectivement inférieurs ou égaux à m, n, p, ...

En particulier, si A est un nombre premier, autre que a, b, c, ..., on aura

$$D(N, A) = 1.$$

La décomposition d'un nombre en ses facteurs n'est possible que d'une seule façon.

Soient

$$N = a^m b^n c^p \ldots$$

et

$$N = a_1^{m'} b_1^{n'} c_1^{p'} \ldots.$$

on aura

$$a^m b^n c^p \ldots = a_1^{m'} b_1^{n'} c_1^{p'} \ldots;$$

donc les nombres a_1, b_1, c_1 se retrouvent dans les nombres a, b, c, ...
Soient

$$a = a_1, \qquad b = b_1, \qquad c = c_1.$$

On notera de plus que m n'est pas supérieur à m', de même que m' n'est pas supérieur à m; donc $m = m'$, de même que $n = n'$, etc.

8. Une racine $k^{\text{ième}}$ d'un nombre n'est rationnelle que si tous les exposants dans la décomposition $a^m b^n c^p \ldots$ sont divisibles par k.

En effet, soit

$$\sqrt[k]{N} = a^{m'} b^{n'} c^{p'} \ldots, \qquad \text{d'où} \qquad N = a^{km'} b^{kn'} c^{kp'} \ldots = a^m b^n c^p \ldots,$$

ce qui entraîne

$$m = km', \qquad n = kn', \qquad p = kp', \qquad \ldots.$$

9. *Dans toute progression arithmétique de n termes*

$$a, \quad a + d, \quad a + 2d, \quad \ldots, \quad a + (n-1)d,$$

où a et d sont premiers avec n, il existe un et un seul terme divisible par n, les autres termes donnent des restes différents quand on les divise par n.

Soient q_1, q_2, q_3, ..., q_n les quotients et r_1, r_2, ..., r_n les restes de la division de termes de la progression arithmétique donnée par n.

Nous allons d'abord prouver que tous les restes sont différents.

Si, en effet, il existait deux restes identiques, $r_k = r_l$ avec k et l inférieurs à N, on aurait

$$a + (k - 1)d = nq_k + r_k, \qquad a + (l - 1)d = nq_l + r_l$$

ou, par soustraction,

$$(k - l)d = n(q_k - q_l).$$

Or, cette égalité n'est pas possible, car k et l étant inférieurs à n, $k - l$ n'est pas divisible par n; d est aussi premier avec n.

Puisque tous les restes sont différents, la série de n restes r_1, $r_2, \ldots, r_n$ ne diffère de la série $0, 1, 2, \ldots, (n-1)$ que par l'ordre des termes. Il n'existe donc qu'*un* et qu'un seul terme divisible par n; tous les autres termes donnent des restes différents si on les divise par n.

10. Proposons-nous de déterminer la plus grande puissance d'un nombre premier A donné qui divise

$$n = 1.2.3\ldots n \qquad (n > \mathrm{A}).$$

Convenons de représenter par $\mathrm{E}(x)$ le plus grand nombre entier contenu dans x. Ainsi,

$$\mathrm{E}(10) = 10, \qquad \mathrm{E}\sqrt{15} = 3.$$

Parmi les n facteurs qui forment le produit $n!$, il y a $\mathrm{E}\left(\frac{n}{\mathrm{A}}\right) = \mathrm{K}$ termes divisibles par A. Ce sont les termes

$$\mathrm{A}, \quad 2\mathrm{A}, \quad 3\mathrm{A}, \quad \ldots, \quad (\mathrm{K}-1)\mathrm{A}, \mathrm{KA}.$$

Parmi ces $\mathrm{E}\left(\frac{n}{\mathrm{A}}\right)$ termes, il y en a $\mathrm{E}\left(\frac{\mathrm{K}}{\mathrm{A}}\right) = \mathrm{E}\left(\frac{n}{\mathrm{A}^2}\right)$ qui sont divisibles non seulement par A, mais aussi par A^2.

On trouvera de même $\mathrm{E}\left(\frac{n}{\mathrm{A}^3}\right)$ termes divisibles par A^3, $\mathrm{E}\left(\frac{n}{\mathrm{A}^4}\right)$ termes divisibles par A^4, etc.

Ainsi n sera divisible par A^m avec

$$m = \mathrm{E}\left(\frac{n}{\mathrm{A}}\right) + \mathrm{E}\left(\frac{n}{\mathrm{A}^2}\right) + \mathrm{E}\left(\frac{n}{\mathrm{A}^3}\right) + \ldots$$

Comme cas particulier, posons

$$n = 2^k, \qquad a = 2.$$

On aura

$$m = 2^{k-1} + 2^{k-2} + 2^{k-3} + \ldots + 2 + 1 = 2^k - 1.$$

On trouve de même pour $n = 2^k - 1$, $a = 2$,

$$m = (2^k - 1) - k = 2^k - (k+1).$$

11. Si N est décomposé en ses facteurs $N = a^m b^n c^p \ldots$, le nombre de diviseurs de N est

$$(m+1)(n+1)(p+1)\ldots;$$

leur somme est

$$S = \frac{a^{m+1}-1}{a-1} \frac{b^{n+1}-1}{b-1} \frac{c^{p+1}-1}{c-1} \cdots.$$

En effet, tout nombre de la forme $a^{m'} b^{n'} c^{p'} \ldots$ sera diviseur de N si $0 < m' < m$, $0 < n' < n$, $0 < p' < p$, ...

Il en résulte que chacun des termes du produit

$$(1 + a + a^2 + \ldots + a^m)(1 + b + b^2 + \ldots + b^n)(1 + c + \ldots + c^p)$$

est diviseur de N, et inversement, tout diviseur de N est un terme de ce produit. Le nombre de diviseurs est donc le nombre de termes de ce produit ou

$$(m+1)(n+1)(p+1)\ldots.$$

La somme de tous les diviseurs est ce produit lui-même, ou

$$S = \frac{a^{m+1}-1}{a-1} \frac{b^{m+1}-1}{b-1} \frac{c^{m+1}-1}{c-1} \cdots.$$

Remarque. — Nous avons dans ce paragraphe compté parmi les diviseurs de N les nombres 1 et N.

Dans quelques problèmes on ne compte pas le nombre N parmi les diviseurs.

Applications. — 1° Trouver la somme des $k^{\text{ièmes}}$ puissances des diviseurs d'un nombre donné $N = a^m b^n c^p \ldots$.

Cette somme est le produit

$$(1 + a^k + a^{2k} + \ldots + a^{mk})(1 + b^k + b^{2k} + \ldots + b^{nk})(1 + c^k + c^{2k} + \ldots + c^{pk})$$

ou

$$\frac{a^{(m+1)k}-1}{a^k-1}\,\frac{b^{(n+1)k}-1}{b-1}\,\frac{c^{(p+1)k}-1}{c-1}\cdots.$$

2° Trouver le plus petit nombre admettant le nombre donné de diviseurs, par exemple 24.

Soit $N = a^m b^n c^p\ldots$ le nombre cherché. On aura

$$(m+1)(n+1)(p+1)\ldots = 24,$$

d'où les solutions possibles :

$m+1=24,$		$n=p=\ldots=0$	et	$N=a^{23};$
$m+1=12,$	$n+1=2,$	$p=q=\ldots=0,$		$N=a^{11}b;$
$m+1=8,$	$n+1=3,$			$N=a^7b^2;$
$m+1=6,$	$n+1=4,$			$N=a^5b^3;$
$m+1=6,$	$n+1=2,$	$p+1=2,$	$q=\ldots=0,$	$N=a^5bc;$
$m+1=4,$	$n+1=3,$	$p+1=2,$		$N=a^3b^2c;$
$m+1=3,$	$n+1=2,$	$p+1=2,$	$q+1=2,$	$N=a^2bcd.$

Le plus petit nombre s'obtient par la forme

$$N = a^3b^2c \quad \text{avec} \quad a=2, \quad b=3, \quad c=5,$$

d'où

$$N = 360.$$

3° Trouver la somme de tous les diviseurs du nombre $N = 2^n$. On trouve

$$S = 2^{n+1}-1 = 2N-1.$$

4° Trouver la somme de tous les diviseurs du nombre

$$N = 2^{n-1}(2^n-1)$$

en supposant 2^n-1 premier; on a

$$S = \frac{2^n-1}{2-1}\,\frac{(2^n-1)^2-1}{(2^n-1)-1} = 2^n(2^n-1) = 2N.$$

12. *Nombres parfaits.* — Nous venons de trouver que si

$$N = 2^{n-1}(2^n-1),$$

on a

$$S = 2N$$

si, toutefois, le nombre 2^n-1 est premier.

Il en résulte que si l'on ne compte pas le nombre N parmi les diviseurs du nombre N, on aura

$$S = 2N - N = N$$

et la somme des diviseurs d'un tel nombre sera égale à ce nombre.

Un tel nombre est dit *parfait*.

Dans le second Volume de ce Livre nous donnerons plus de détails sur les nombres parfaits. Actuellement, bornons-nous à remarquer que les nombres parfaits pairs sont tous de la forme

$$2^{n-1}(2^n - 1)$$

avec la condition que $2^n - 1$ soit premier. On ne connaît pas de nombres parfaits impairs. Pour ce qui est des nombres parfaits pairs, on en connaît les douze suivants qui correspondent à

$$n = 2.3.5.7.13.17.19.31.61.89.107 \quad \text{et} \quad 127$$

dans la formule

$$N = 2^{n-1}(2^n - 1).$$

Les sept premiers sont connus depuis assez longtemps. Euler (1772) a vérifié le cas de $n = 31$, Seelhof (1886) a donné le cas de $n = 61$, Powers (1911) a établi la primalité de $2^{89} - 1$, Powers et Fauquembergue (1914) ont trouvé le cas de $n = 107$ et, enfin, Fauquembergue (1914) a trouvé le nombre parfait correspondant à $n = 127$.

13. *Nombres amiables.* — Considérons deux nombres tels que

$$N_1 = 220 = 22.5.11$$

et

$$N_2 = 284 = 2^2.71.$$

Soit S_1 et S_2 la somme de leurs diviseurs en exceptant le nombre N_1 ou N_2 du nombre des diviseurs. On trouve :

$$S_1 = (2^3 - 1)(5 + 1)(11 + 1) - N_1 = 504 - N_1 = 284 = N_2,$$
$$S_2 = 7.72 - N_2 = 504 - N_2 = N_1.$$

Ainsi ces deux nombres sont tels que la somme des diviseurs de chacun d'eux est égale à l'autre.

Des nombres semblables sont dits *nombres amiables*. Nous en

donnerons une théorie plus détaillée dans le deuxième volume de cet Ouvrage.

14. Soit à déterminer de combien de manières on peut décomposer un nombre donné $N = a^m b^n c^p \ldots$ en produit de deux facteurs.

Désignons par K le nombre des diviseurs

$$K = (m+1)(n+1)(p+1)\ldots,$$

et supposons en premier lieu que le nombre donné n'est pas carré parfait, c'est-à-dire qu'au moins un des nombres m, n, p est impair et K est par conséquent pair.

Le nombre des décompositions possibles est alors évidemment de

$$\frac{1}{2}K = \frac{1}{2}(m+1)(n+1)(p+1)\ldots.$$

Si, en second lieu, le nombre donné est un carré parfait, le nombre des décompositions possibles est de

$$\frac{1}{2}(1+K) = \frac{1}{2}[1+(m+1)(n+1)(p+1)\ldots].$$

15. On appelle *indicateur* de N et l'on désigne par $\varphi(N)$ le nombre de nombres plus petits que N et premiers avec lui. Ainsi $\varphi(6) = 2$, car il n'y a que deux nombres plus petits que 6 et premiers avec 6 (1 et 5).

Dans cette question le nombre 1 est considéré comme étant premier avec n'importe quel nombre.

Si N est un nombre premier, on a

$$\varphi(N) = N - 1.$$

En effet, tous les nombres 1, 2, 3, ..., $(N-1)$ sont inférieurs à N et premiers avec lui.

Si $N = a^m$, a étant un nombre premier :

$$\varphi(N) = a^{m-1}(a-1).$$

En effet, seuls les nombres a, $2a$, $3a$, ..., $(a^{m-1}-1)a$, parmi les nombres 1, 2, 3, ..., $(N-1)$, ne sont pas premiers avec N; donc :

$$\varphi(N) = N - 1 - (a^{m-1} - 1) = a^m - a^{m-1} = a^{m-1}(a-1).$$

16. Théorème. — *Si* $D(A, B) = 1$, *on a*

$$\varphi(AB) = \varphi(A)\varphi(B).$$

Soient $a_1, a_2, a_3, \ldots, a_m$ tous les nombres inférieurs à A et premiers avec lui, et $b_1, b_2, b_3, \ldots, b_n$ tous les nombres inférieurs à B et premiers avec lui.

Pour avoir tous les nombres inférieurs à AB et premiers avec AB, formons le tableau :

$$\begin{array}{ccccc}
a_1, & a_2, & a_3, & \ldots, & a_m, \\
A + a_1, & A + a_2, & A + a_3, & \ldots, & A + a_m, \\
2A + a_1, & 2A + a_2, & 2A + a_3, & \ldots & 2A + a_m, \\
3A + a_1, & 3A + a_2, & 3A + a_3, & \ldots, & 3A + a_m, \\
\ldots\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\
(B-1)A + a_1, & (B-1)A + a_2, & (B-1)A + a_3, & \ldots, & (B-1)A + a_m.
\end{array}$$

Chaque colonne contient B termes qui forment une progression arithmétique dont la raison est A, nombre premier avec le premier terme $a_i (i = 1, 2, 3, \ldots)$ et avec B. Si l'on divise chacun des termes de ce tableau par B, on obtient dans chaque colonne les restes

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad \ldots, \quad (B-1).$$

Seul l'ordre de ces restes différera d'une colonne à l'autre.

Remarquons encore que tous les termes de ce tableau sont premiers avec A. Et si l'on élimine de ce tableau les nombres qui ne sont pas premiers avec B, on aura tous les nombres inférieurs à AB et premiers avec AB.

Or, dans chaque colonne, seuls les restes (de la division par B)

$$b_1, \quad b_2, \quad b_3, \quad \ldots, \quad b_n$$

ne sont pas à éliminer. Il en résulte que le nombre total des nombres inférieurs à AB et premier avec AB ou $\varphi(AB)$ est le produit $\varphi(A)\varphi(B)$, le premier de ces facteurs est le nombre de termes de chaque ligne, le second est le nombre de termes qui restent non éliminés dans chaque colonne.

17. Par les considérations qui précèdent (I, 15, 16) nous pouvons trouver l'indicateur de n'importe quel nombre, si l'on connaît la décomposition de ce nombre.

Soit

$$N = a^m b^n c^p \ldots,$$

$a, b, c, \ldots$ étant supposés différents, donc premiers entre eux. On a

$$\varphi(a^m) = a^{m-1}(a-1),$$
$$\varphi(b^n) = b^{n-1}(b-1),$$
$$\varphi(c^p) = c^{p-1}(c-1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

d'où

$$\varphi(a^m b^n c^p \ldots) = a^{m-1} b^{n-1} c^{p-1}(a-1)(b-1)(c-1)$$

ou

$$\varphi(N) = a^{m-1} b^{n-1} c^{p-1}(a-1)(b-1)(c-1)\ldots$$
$$= a^m b^n c^p\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)$$
$$= N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots.$$

Cette dernière formule peut être obtenue directement de la manière suivante :

La suite

$$1.2.3.4.5\ldots N$$

contient N nombres non supérieurs à N.

Pour avoir les nombres inférieurs à N et premiers avec lui, il suffit d'éliminer de cette suite tous les nombres non premiers avec $a, b, c, \ldots$. Or, a étant un nombre premier, seuls les nombres

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad \left(\frac{N}{a}\right)a$$

ne sont pas premiers avec a. Leur nombre est de $\frac{N}{a}$.

La suite primitive 1, 2, 3, 4, ..., N ne contiendra plus après élimination que les

$$N' = N - \frac{N}{a} = N\left(1-\frac{1}{a}\right) \text{ nombres}$$

$$1.2.3\ldots a-1, \quad a+1\ldots 2a-1, \quad 2a+1\ldots N-1.$$

Ces N' nombres peuvent être distribués en $\frac{N'}{b}$ progressions de b termes chacune, la raison de la progression étant a qui est premier avec b. Chaque progression contiendra *un* et un seul terme non

premier avec b (divisible par b). Ces termes sont à éliminer, car ils ne sont pas premiers avec N.

Après cette élimination, il restera

$$N'' = N' - \frac{N'}{b} = N'\left(1 - \frac{1}{b}\right) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$$

termes premiers avec a et b, donc avec ab ou $a^m b^n$.

Ces N'' nombres peuvent à leur tour être distribués en $\frac{N''}{c}$ progressions de c termes chacune. Chaque progression contiendra un et un seul terme divisible par c, donc non premier avec c et qui est à éliminer. Il restera

$$N''' = N'' - \frac{N''}{c} = N''(1 - c) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)$$

termes non divisibles ni par a, ni par b, ni par c, donc premiers avec abc ou $a^m b^n c^p$ ou avec N.

D'où

$$\varphi(N) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right).$$

Applications :

$$\varphi(4n) = 2\varphi(2n),$$
$$\varphi(4n + 2) = \varphi(2n + 1),$$
$$\varphi(2^m) = 2^{m-1},$$
$$\varphi(3^m) = 2.3^{m-1},$$
$$\varphi(30) = 8,$$
$$\varphi(210) = 48,$$
$$\varphi(30030) = 5760.$$

18. Soit à déterminer le nombre des nombres premiers avec N et dont le plus grand commun diviseur avec N est A.

Remarquons d'abord que le nombre A donné doit être un diviseur de N.

Soient ensuite $Ax_1, Ax_2, Ax_3, \ldots, Ax_n$ les nombres cherchés.

Puisque $Ax_i (i = 1, 2, 3, \ldots)$ est inférieur à N, on aura

$$X_i < \frac{N}{A}.$$

Ensuite, $D(Ax_i, N) = A$ donne

$$D\left(X_i \frac{N}{A}\right) = 1;$$

donc tous les nombres X_i inférieurs à $\frac{N}{A}$ et premiers avec $\frac{N}{A}$ peuvent être employés.

Leur nombre est donc

$$\varphi\left(\frac{N}{A}\right).$$

19. *Si* $a_1, a_2, a_3, \ldots, a_k$ *sont tous les diviseurs du nombre* $N = a^m b^n c^p \ldots$ [*donc* $k = (m+1)(n+1)(p+1)\ldots$], *on a*

$$\varphi(a_1) + \varphi(a_2) + \varphi(a_3) + \ldots + \varphi(a_k) = N.$$

En effet, distribuons les N nombres 1, 2, 3, ..., N en k séries, de sorte que les termes de chaque série aient le même plus grand commun diviseur $a_i (i = 1, 2, 3, \ldots, k)$ avec N.

On aura alors, en vertu du paragraphe précédent,

$$\varphi\left(\frac{N}{a_1}\right) + \varphi\left(\frac{N}{a_2}\right) + \varphi\left(\frac{N}{a_3}\right) + \ldots + \varphi\left(\frac{N}{a_k}\right) = N;$$

or, $\frac{N}{a_i}(i = 1, 2, 3, \ldots, k)$ est aussi un diviseur

$$a_j (j = 1, 2, 3, \ldots, k);$$

donc

$$\varphi(a_1) + \varphi(a_2) + \varphi(a_3) + \ldots + \varphi(a_k) = N.$$

Remarquons, toutefois, qu'il est essentiel de poser $\varphi(1) = 1$ pour que la formule ne soit pas en défaut.

Corollaire. — *Si* p *est un nombre premier et* $a_1, a_2, \ldots, a_k$ *tous les diviseurs de* $p - 1$, *on aura*

$$\varphi(p) = \varphi(a_1) + \varphi(a_2) + \varphi(a_3) + \ldots + \varphi(a_k).$$

CHAPITRE II.

CONGRUENCE DU PREMIER DEGRÉ.

1. Deux nombres a et b sont dits *congrus* au module m quand leur différence $a - b$ est divisible par m.

On écrit

$$a \equiv b \pmod{m}.$$

Cela veut dire que les nombres a et b divisés par m donnent le même reste.

Il résulte de la définition que tout nombre N est congru avec O quand on prend pour module un diviseur quelconque de N. Ainsi

$$\mathrm{A}k \equiv 0 \pmod{\mathrm{A}}.$$

Le dividende est congru avec le reste, quand on prend pour module le diviseur (ou le quotient).

Si $\mathrm{A} = \mathrm{B}q + r$, on a

$$\mathrm{A} \equiv r \pmod{\mathrm{B}} \quad \text{et} \quad \mathrm{A} \equiv r \pmod{q}.$$

En effet, la différence $\mathrm{A} - r$ ou $\mathrm{B}q$ est divisible par B et par q.

Deux nombres quelconques sont congrus quand on prend pour module un diviseur quelconque de leur différence.

2. Propriétés des congruences. — 1° *Deux congruences de même module peuvent être ajoutées (algébriquement) membre à membre.*

Si $\mathrm{A} \equiv a$ et $\mathrm{B} \equiv b \pmod{m}$, on a aussi

$$\mathrm{A} \pm \mathrm{B} \equiv a \pm b \pmod{m}.$$

En effet, la divisibilité de $\mathrm{A} - a$ et $\mathrm{B} - b$ par m entraîne celle de

$$(\mathrm{A} - a) \pm (\mathrm{B} - b) \quad \text{ou} \quad (\mathrm{A} \pm \mathrm{B}) - (a \pm b),$$

ce qui s'exprime par

$$A \pm B \equiv a \pm b \pmod{m}.$$

2° *Deux nombres congrus avec un même troisième et pour un même module sont congrus entre eux.*

Si $A \equiv a$ et $B \equiv a \pmod{m}$, on aura

$$A \equiv B \pmod{m}.$$

En effet, $A - a$ et $B - a$ étant divisibles par m, leur différence $A - B$ l'est aussi, donc $A \equiv B \pmod{m}$.

3° *Une congruence ne change pas, si l'on ajoute aux deux membres la même quantité (positive ou négative).*

Si $A \equiv a \pmod{m}$, on a

$$A \pm K \equiv a \pm K \pmod{m}.$$

En effet, la différence $(A \pm K) - (a \pm K)$ ne diffère pas de la différence $A - a$.

Il résulte de là que les termes d'une congruence peuvent être transportés d'un membre de la congruence dans l'autre, en changeant les signes de ces termes, tout à fait comme s'il s'agissait d'une équation.

4° *Les termes d'une congruence peuvent être multipliés par un même nombre.*

Si $A \equiv a \pmod{m}$ on a

$$KA \equiv Ka \pmod{m}.$$

En effet, la différence $KA - Ka = K(A - a)$ est divisible par $A - a$, donc par m qui est diviseur de $A - a$.

5° *Deux congruences d'un même module peuvent être multipliées membre à membre.*

Si $A \equiv a$ et $B \equiv b \pmod{m}$, on a

$$AB \equiv ab.$$

En effet, les différences $A - a$ et $B - b$ étant divisibles par m, désignons par x et y les quotients, de sorte que

$$A - a = mx \quad \text{et} \quad B - b = my$$

ou

$$A = mx + a \qquad \text{et} \qquad B = my + b,$$

d'où

$$AB = (mx + a)(my + b) = m^2xy + m(bx + ay) + ab,$$

d'où il résulte que la différence

$$AB - ab = m^2xy + m(bx + ay)$$

est divisible par m, ce qu'on peut exprimer par la congruence

$$AB \equiv ab \pmod{m}.$$

6° *Si* $A \equiv a$ *et* $B \equiv b$ (mod m), *on aura aussi*

$$A^n B^p \equiv a^n b^p \pmod{m}.$$

En effet, la congruence $A \equiv a \pmod{m}$ entraîne celle de $A^n \equiv a^n \pmod{m}$ (par une répétition successive d'une multiplication de deux congruences ou simplement en remarquant que la différence $A^n - a^n$ est divisible par $A - a$, donc par m).

De même, la congruence $B \equiv b \pmod{m}$ entraîne celle de $B^p \equiv b^p$. Ces dernières congruences, multipliées membre à membre, donnent

$$A^n B^p \equiv a^n b^p.$$

7° *On peut diviser les termes d'une congruence par tout diviseur premier avec le module.*

Si K et m sont premiers entre eux et $AK \equiv aK \pmod{m}$, on aura

$$A \equiv a \pmod{m}.$$

En effet, $AK - aK = (A - a)K$ étant divisibles par m, et K étant premier avec m, $A - a$ est aussi divisible par m; donc

$$A \equiv a \pmod{m}.$$

8° *Un diviseur commun de deux membres de la congruence et du module peut être écarté.*

Si $KA \equiv Ka$ (mod $m = Kp$), on aura

$$A \equiv a \pmod{p}.$$

En effet, $(KA - Ka) = K(A - a)$ étant divisible par $m = Kp$,

il en résulte que $A - a$ est divisible par p ou que

$$A \equiv a \pmod{p}.$$

9° *Si $f(x)$ est une fonction algébrique avec des coefficients entiers et $a \equiv b \pmod{m}$, on aura*

$$f(a) \equiv f(b) \pmod{m}.$$

En effet, posons

$$f(x) = Ax^n + Bx^{n-1} + \ldots + Ex + F;$$

la congruence $a \equiv b \pmod{m}$ entraîne les suivantes :

$$\begin{aligned} Aa^n &\equiv Ab^n \pmod{m}, \\ Ba^{n-1} &\equiv Bb^{n-1}, \\ \ldots&\ldots\ldots, \\ Ea &\equiv Eb, \\ F &\equiv F. \end{aligned}$$

En ajoutant ces congruences membre à membre, on obtient

$$f(a) \equiv f(b).$$

10° *Deux nombres congrus suivant deux modules premiers entre eux sont congrus suivant un module égal à leur produit.*

Si $A \equiv a \pmod{m}$ et $A \equiv a \pmod{n}$, m et n étant premiers entre eux, on aura

$$A \equiv a \pmod{mn}.$$

En effet, $A - a$ étant divisible par m et n qui sont premiers entre eux, $A - a$ sera divisible par le produit mn ou

$$A \equiv a \pmod{mn}.$$

3. Nous avons vu que tout nombre est congru avec le reste de la division de ce nombre par le module.

Si donc le reste de la division de A par m est r, le quotient étant désigné par q, on aura

$$A \equiv r \pmod{m}.$$

Puisque le reste d'une division est toujours inférieur au diviseur,

il en résulte qu'on peut toujours trouver un nombre inférieur au module et congru avec le nombre donné.

On peut maintenant distinguer deux cas :

1° $r > \frac{m}{2}$. Si alors on remplace q par $q+1$ et le reste positif r par le reste négatif $r' = r - m$, on aura

$$r' < \frac{m}{2};$$

2° Si $r < \frac{m}{2}$, on aura

$$r' > \frac{m}{2}.$$

Dans les deux cas, il existe :

1° Un nombre positif compris entre o et m et congru avec le nombre donné suivant le module m;

2° Un nombre positif ou négatif inférieur à $\frac{m}{2}$ et congru avec le nombre donné suivant le module m.

Le premier reste ou résidu est le reste du nombre considéré (mod m); le deuxième reste est le résidu minimum du nombre considéré (mod m).

Exemples :

$$110 \equiv 6 \pmod{13},$$

6 est le résidu du nombre 110 (mod 13); c'est aussi le résidu minimum;

$$10^{2n+1} \equiv +10 \equiv -1 \pmod{11},$$

10 est le résidu de 10^{2n+1}, -1 est le résidu minimum du nombre considéré (mod 11).

4. Théorème. — *Si m est un nombre impair, et a la valeur absolue du résidu minimum de* A (mod m), *le signe de a est déterminé par le signe de la quantité*

$$(-1)^{E\frac{2A}{m}},$$

$E\left(\frac{2A}{m}\right)$ *désignant le plus grand entier contenu dans* $\left(\frac{2A}{m}\right)$.

En effet, si q est le quotient de la division de A par m, on peut

avoir deux cas :

1° $q < \frac{A}{m} < q + \frac{1}{2}$, alors

$$2q < \frac{2A}{m} < 2q+1 \quad \text{et} \quad E\left(\frac{2A}{m}\right) = 2q;$$

le résidu minimum de A (mod m) sera positif.

2° $q + \frac{1}{2} < \frac{A}{m} < q+1$, alors

$$2q+1 < A < 2q+2 \quad \text{et} \quad E\left(\frac{2A}{m}\right) = 2q+1,$$

et le résidu minimum de A (mod m) sera négatif.

On aura donc toujours :

$$\text{résidu minimum de A(mod } m) = (-1)^{E\frac{2A}{m}} a,$$

a étant la valeur absolue du résidu minimum.

5. Si dans l'expression de

$$f(x) = Ax^m + Bx^{m-1} + \ldots + Ex + F,$$

où les coefficients A, B, C, ... sont des entiers (positifs ou négatifs), on remplace x par les valeurs

$$0.1.2.3\ldots k\ldots m\ldots m+k\ldots,$$

et l'on calcule les valeurs

$$f(0), \quad f(1), \quad f(2), \quad \ldots, \quad f(m), \quad \ldots, \qquad (\text{mod } m),$$

la suite ainsi obtenue est périodique, car

$$f(m+k) \equiv f(k) \quad (\text{mod } m).$$

Ainsi, si par exemple $f(x) = x^3 - 8x + 6$ et $m = 5$, on aura

$$x = 0.1.2.3.4.5.6.7.8\ldots,$$
$$f(x) \equiv 1.4.3.4.3.1.4.3.4\ldots \qquad (\text{mod } 5).$$

Dans le cas envisagé, la période est (1.4.3.4.3).

Dans la suite des valeurs de x, on ne rencontre point les valeurs $f(x) \equiv 0$ ni $f(x) \equiv 2$; conséquemment, les congruences

$$x^3 - 8x + 6 \equiv 0 \quad \text{ou} \quad x^3 - 8x + 6 \equiv 2 \qquad (\text{mod } 5)$$

n'ont pas de solution.

A fortiori, les équations

$$x^3 - 8x + 6 = 0 \qquad \text{et} \qquad x^3 - 8x + 6 = 2$$

n'ont pas de racines rationnelles.

6. Des propriétés fondamentales des congruences résulte la possibilité de les utiliser pour la vérification des opérations de calcul.

Ainsi, si le résultat d'une opération quelconque sur les nombres A, B, C, ... nous a conduits au résultat X,

$$X = F(A, B, C, \ldots).$$

Si l'on désigne par x, a, b, c, ... les résidus des nombres X, A, B, C, ... (mod m), on doit avoir

$$x \equiv F(a, b, c, \ldots) \pmod{m}.$$

Parfois le calcul par congruence est non seulement plus simple que le calcul de valeur absolue, mais indispensable.

Ainsi, soit à trouver, par exemple, le reste de la division 2^{2048} par 974849. Le nombre 2^{2048} aurait contenu plus de 600 chiffres. Rien qu'exprimer ce nombre en système décimal est difficile, mais il est relativement facile de trouver le reste demandé de la division 2^{2048} par 974849 sans avoir le dividende explicitement.

On trouve :

$$\begin{aligned}
2^{16} &\equiv 65536, \\
2^{32} &\equiv 65536^2 \equiv -217398 \pmod{974849} \\
2^{64} &\equiv 217398^2 \equiv 236035, \\
2^{128} &\equiv 236035^2 \equiv -99125, \\
2^{256} &\equiv 99125^2 \equiv 262554, \\
2^{512} &\equiv 262554^2 \equiv 105576, \\
2^{1024} &\equiv 105576^2 \equiv 501577, \\
2^{2048} &\equiv 501577^2 \equiv -1.
\end{aligned}$$

Puisque $2^{2048} \equiv -1 \pmod{974849}$, on aura

$$2^{2048} + 1 \equiv 0 \pmod{974849},$$

ce qui exprime que $2^{2048} + 1$ est divisible par 974849.

Ce résultat infirme encore le théorème de Fermat (I, 4).

Voici tous les résultats connus à ce jour :

$n =$ 5.	$F_n = 2^{2^n} + 1 =$	641.6700417
6.	»	274177.67280421310721
7. 8.	Les nombres correspondants sont composés, mais on ne connaît pas les facteurs de ces nombres.	
9.	F_n est divisible par	$2^{16}.37 + 1$
11.	»	$2^{13}.3.13 + 1$ et $2^{13}.7.17 + 1$
12.	»	$2^{14}.7 + 1, 2^{16}.397 + 1$ et $2^{16}.7.139 + 1$
18.	»	$2^{20}.13 + 1$
23.	»	$2^{25}.5 + 1$
36.	»	$2^{39}.5 + 1$
38.	»	$2^{41}.3 + 1$
73.	»	$2^{75}.5 + 1$

Le premier résultat est d'Euler (1732), le second de Landry (1880), les deux suivants de Morehead et Western (1909). Le résultat pour $n = 9$ est encore de Western (1903), ceux qui correspondent à $n = 11$ sont de Cunningham (1899). Pour $n = 12$, le premier facteur est de Lucas et Pervouchine (1878), les deux autres de Western (1903). C'est encore M. Western qui a trouvé les résultats pour $n = 18$ (1903). Le cas de $n = 23$ est de Pervouchine (1878). Seelhoff (1886) a trouvé le facteur pour $n = 36$. Cunningham, Cullen et Western ont trouvé le facteur pour $n = 38$. Enfin, M. Morehead (1906) a trouvé le facteur pour $n = 73$.

Le nombre $2^{2^{73}} + 1$ est donc divisible par $5.2^{75} + 1$.

Le nombre $2^{2^{73}} + 1$ est tellement grand qu'il est impossible de l'écrire explicitement dans le système décimal. Il aurait contenu

$$0,3 \times 9444 \times 10^{18}, \quad \text{soit plus de} \quad 2700 \times 10^{18} \text{ chiffres.}$$

Avec des chiffres de 1^{mm} de largeur, la bande qui le contiendrait aurait 2700×10^{12} kilomètres de longueur et ferait plus de 60×10^9 fois le tour de l'équateur terrestre.

A raison d'un chiffre par seconde, 10 heures de travail par jour et 360 jours ouvrables par an, il faudrait travailler pendant

$$\frac{2700 \times 10^{18}}{60 \times 60 \times 10 \times 360} = 2 \times 10^{14} \text{ ans}$$

rien que pour recopier ce nombre.

Si toute la population de la Terre ($1,5 \times 10^9$ habitants) était occupée uniquement à recopier ce nombre, supposé écrit en système décimal, on aurait une besogne qui durerait

$$\frac{2 \times 10^{14}}{1.5 \times 10^9} = 130000 \text{ années.}$$

Ces considérations montrent que le calcul par congruence est une véritable nécessité pour obtenir des résultats qu'on ne peut pas aborder autrement.

7. Le nombre des congruences possibles suivant un module déterminé est limité. Ainsi, suivant le module m, tout nombre A est congru avec un des nombres de la suite $0.1.2.3\ldots(m-1)$.

Il n'existe donc que m congruences différentes (mod m).

En d'autres termes, tout nombre A est un multiple de m, augmenté d'un nombre de la suite $0.1.2.3.4\ldots(m-1)$. On dit encore que, suivant le module m, les nombres se subdivisent en m classes :

1°	Nombres de la forme	Km	ou	$\equiv 0$	(mod m)
2°	»	$Km+1$	»	$\equiv 1$	»
3°	»	$Km+2$	»	$\equiv 2$	»
...	...	...	...	...	...
m^o	»	$Km+(m-1)$	»	$\equiv m-1$	»

Ainsi, suivant le module 5, on aura les cinq classes :

1°	Nombres de la forme	5K	ou	$\equiv 0$	(mod 5)
2°	»	5K + 1	»	$\equiv 1$	»
3°	»	5K + 2	»	$\equiv 2$	»
4°	»	5K + 3	»	$\equiv 3$	»
5°	»	5K + 4	»	$\equiv 4$	»

8. Nous avons vu (II, 5) que la suite $f(x)$ est périodique quand on remplace x par la série des nombres naturels, donc si $x=r$ satisfait à la congruence $f(x) \equiv 0 \pmod m$,

$$x = Km + r \quad \text{ou} \quad x \equiv r \pmod m$$

satisfait aussi à cette congruence. Toutes ces solutions ne seront comptées que pour une solution. Nous pouvons donc dire que la congruence

$$f(x) \equiv 0 \pmod m$$

a autant de solutions différentes qu'il y a de nombres dans la suite $0.1.2.3\ldots(m-1)$ qui lui satisfont.

Ainsi la congruence $x^2 \equiv 5 \pmod{31}$ a deux solutions :

$$x \equiv 6 \quad \text{et} \quad x \equiv 25 \pmod{31}.$$

La congruence $x^3 \equiv 2 \pmod{11}$ n'a qu'une solution :

$$x \equiv 7 \pmod{11}.$$

La congruence $x^3 \equiv 2 \pmod 7$ est impossible.

9. Abordons maintenant la résolution d'une congruence du premier degré à une inconnue. Une telle congruence peut être mise sous la forme

$$ax \equiv b \pmod m.$$

Remarquons d'abord que la congruence $ax \equiv b \pmod m$ n'est pas possible si a et m ont un diviseur commun qui ne divise pas b. En effet, la divisibilité de $ax - b$ par m peut s'exprimer par

$$ax - b = m\mathrm{K} \quad \text{ou} \quad b = ax - m\mathrm{K}.$$

Il résulte de la dernière égalité que tout diviseur de a et m est aussi un diviseur de b. Dans ce cas, on peut simplifier la congruence (ainsi que le module) par ce diviseur. Nous traiterons ultérieurement ce cas (II, **14**).

Nous allons démontrer que si a et m sont premiers entre eux, la congruence $ax \equiv b \pmod m$ est toujours possible et n'admet qu'une solution.

En effet, la progression

$$0, \quad a, \quad 2a, \quad 3a, \quad \ldots, \quad ra, \quad \ldots, \quad (m-1)a$$

contient un et un seul terme qui est $\equiv b \pmod m$. Si ce terme est ra, de sorte que $ra \equiv b \pmod m$, on aura $x = r$, et d'une façon générale $x \equiv r \pmod m$ comme solution de la congruence

$$ax \equiv b \pmod m.$$

10. On peut trouver cette solution de la manière suivante : Si l'on exprime la fraction $\frac{a}{m}$ en fraction continue, on trouve

$$\frac{a}{m} = r_1 r_2 r_3 \ldots r_n\,;$$

si ensuite on forme les réduites successives, dont la dernière est $\frac{a}{m}$, on a

$$\frac{p_1}{q_1}\ \frac{p_2}{q_2}\ \cdots\ \frac{p_{n-1}}{q_{n-1}}\ \frac{a}{m},$$

d'où

$$a q_{n-1} - m p_{n-1} = (-1)^n,$$

ou

$$a q_{n-1} \equiv (-1)^n \pmod{m},$$

ou, en multipliant par $(-1)^n b$,

$$(-1)^n ab\, q_{n-1} \equiv b \pmod{m},$$

d'où

$$x \equiv (-1)^n b\, q_{n-1} \pmod{m}.$$

Nous verrons dans la suite deux autres solutions de ce problème (III, 4; V, 12).

Exemples. — Soit à résoudre la congruence

$$13x \equiv 6 \pmod{17}.$$

On a

$$\frac{13}{17} = 0, 1, 3, 4.$$

Les réduites sont :

$$\frac{0}{1},\quad \frac{1}{1},\quad \frac{3}{4},\quad \frac{13}{17};$$

d'où

$$13.4 - 17.3 = +1 \qquad \text{ou} \qquad 13.4 \equiv 1 \pmod{17},$$

ou, en multipliant par 6 :

$$13.24 \equiv 6 \pmod{17},$$

d'où

$$x \equiv 24 \equiv 7 \pmod{17}.$$

11. On peut attribuer une signification au symbole $\frac{b}{a}$ de façon à avoir $x \equiv \frac{b}{a} \pmod{m}$ comme solution de la congruence

$$ax \equiv b \pmod{m}.$$

Nous allons adopter la définition suivante :

Si a et m sont premiers entre eux, le symbole $\frac{b}{a} \pmod{m}$ désigne

un nombre entier qui, multiplié par a, donne un nombre

$$\equiv b \pmod{m}.$$

Par cette définition, la solution de la congruence $ax \equiv b \pmod{m}$ est

$$x \equiv \frac{b}{a} \pmod{m}.$$

On peut aussi définir ce symbole en disant que : « diviser b par $a \pmod{m}$ veut dire qu'il faut diviser par a le nombre $b + Km$, K étant convenablement choisi, de façon que $b + Km$ devienne un multiple de a ».

D'après cela, ayant la congruence $13x \equiv 6 \pmod{17}$, on peut écrire

$$x \equiv \frac{16}{13} \equiv \frac{6 + 5.17}{13} \equiv 7 \pmod{17}.$$

12. *Nombres associés.* — On appelle *associé* de $a \pmod{m}$ le nombre α tel que $a\alpha \equiv 1 \pmod{m}$. Les nombres a et m étant supposés premiers entre eux.

Tout nombre autre que $\equiv 0 \pmod{m}$ a son associé, car si a et m sont premiers entre eux, la congruence $ax \equiv 1 \pmod{m}$ est toujours possible.

Ainsi, pour le module 11, les nombres

1 2 3 4 5 6 7 8 9 10

auront pour associés

1 6 4 3 9 2 8 7 5 10

et, pour le module 13, les nombres

1 2 3 4 5 6 7 8 9 10 11 12

auront pour associés

1 7 9 10 8 11 2 5 3 4 6 12.

On notera qu'il n'y a pas d'autre nombre que 1 et $m - 1$ qui soient identiques à leurs associés.

13. Bien que la solution de la congruence $ax \equiv b \pmod{m}$ est générale, il est quelquefois préférable de la remplacer par d'autres congruences si le module m est un nombre composé.

Soit la congruence

$$ax \equiv b \pmod{m = pq}.$$

On la remplacera par les congruences

$$ax \equiv b \pmod{p},$$
$$ax \equiv b \pmod{q}.$$

Bien entendu, dans la congruence $ax \equiv b \pmod{p}$, les nombres a et b seront remplacés par leur reste $(\text{mod}\, p)$. Il en est de même de la deuxième congruence.

Si

$$x \equiv r \pmod{p},$$
$$x \equiv r \pmod{q}$$

sont les solutions de ces congruences, on trouvera un nombre qui est à la fois $\equiv r \pmod{p}$ et $\equiv r' \pmod{q}$ et l'on aura une solution de la congruence donnée.

Exemple :

$$997x \equiv 113 \pmod{720 = 16.9.5}.$$

La congruence donnée devient :

$$5x \equiv 1, \quad \text{d'où} \quad x \equiv 13 \pmod{16};$$
$$7x \equiv 5, \quad \text{»} \quad x \equiv 2 \pmod{9};$$
$$2x \equiv 3, \quad \text{»} \quad x \equiv 4 \pmod{5}.$$

Pour trouver un nombre qui soit $\equiv 13 \pmod{16}$ et $\equiv 2 \pmod{9}$, on opérera de la façon suivante :

Les nombres qui sont $\equiv 13 \pmod{16}$ peuvent s'écrire $16y + 13$; on aura donc

$$16y + 13 \equiv 2 \pmod{9}$$

ou

$$7y \equiv 7 \pmod{9}, \quad \text{d'où} \quad y \equiv 1 \pmod{9}$$

et

$$16y + 13 \equiv 29 \pmod{144}.$$

Ainsi les nombres qui sont $\equiv 29 \pmod{144}$ sont à la fois

$$\equiv 13 \pmod{16} \quad \text{et} \quad \equiv 2 \pmod{9}.$$

Il reste à trouver les nombres qui sont

$$\equiv 29 \pmod{144} \quad \text{et} \quad \equiv 4 \pmod{5}.$$

Les nombres $\equiv 29 \pmod{144}$ s'écrivent $144z + 29$; on aura donc

$$144z + 29 \equiv 4 \pmod 5 \quad \text{où} \quad 4z \equiv 0 \pmod 5,$$

d'où

$$z \equiv 0 \pmod 5$$

et

$$144z + 29 \equiv 29 \pmod{720}.$$

Ainsi, $x \equiv 29 \pmod{720}$ est solution de la congruence donnée.

14. Supposons maintenant que les nombres a, b et n ont un facteur commun k, mais tel que $\frac{a}{k}$ et $\frac{m}{k}$ soient premiers entre eux.

En remplaçant dans $ax \equiv b \pmod m$ les nombres a, b et m par ka', kb' et km', il vient

$$ka'x \equiv kb' \pmod{km'} \quad \text{ou} \quad a'x \equiv b' \pmod{m'}$$

qui donne

$$x \equiv r \quad \left(\bmod\ m' \equiv \frac{m}{k}\right).$$

Cette solution unique $\pmod{m'}$ donne k solutions $\pmod m$:

$$x \equiv r, \quad r + \frac{m}{k}, \quad r + \frac{2m}{k}, \quad \ldots, \quad r + \frac{(k-1)m}{k} \pmod m.$$

Exemple. — La congruence $315x \equiv 110 \pmod{215}$ donne

$$63x \equiv 22 \pmod{43} \quad \text{ou} \quad x \equiv 14 \pmod{43},$$

ou

$$x \equiv 14, 57, 100, 143, 186 \pmod{215}$$

15. Supposons maintenant qu'il s'agisse de résoudre simultanément plusieurs congruences :

$$a_1x \equiv b_1 \pmod{m_1},$$
$$a_2x \equiv b_2 \pmod{m_2}, \quad \ldots, \quad a_nx \equiv b_n \pmod{m_n}.$$

Les congruences $\pmod m$, dans lesquelles le module m n'est pas premier, seront remplacées par les congruences des modules m', m'', m''', ..., dans lesquelles les modules sont premiers entre eux (III, 13). On aura ainsi le système :

$$a'_1x \equiv b'_1 \pmod{m'_1}, \quad a'_2x \equiv b'_2 \pmod{m'_2}, \quad \ldots, \quad a'_nx \equiv b'_n \pmod{m'_n};$$
$$a''_1x \equiv b''_1 \pmod{m''_1}, \quad a''_2x \equiv b''_2 \pmod{m''_2}, \quad \ldots, \quad a''_nx \equiv b''_n \pmod{m''_n};$$
$$\ldots\ldots\ldots\ldots, \quad \ldots\ldots\ldots\ldots, \quad \ldots, \quad \ldots\ldots\ldots\ldots$$

En résolvant chacune de ces congruences, on obtient :

$$x \equiv r'_1 \pmod{m'_1}, \quad x \equiv r'_2 \pmod{m'_2}, \quad \ldots, \quad x \equiv r'_n \pmod{m'_n};$$
$$x \equiv r''_1 \pmod{m''_1}, \quad x \equiv r''_2 \pmod{m''_2}, \quad \ldots, \quad x \equiv r''_n \pmod{m''_n};$$
$$\ldots\ldots\ldots, \quad \ldots\ldots\ldots, \quad \ldots, \quad \ldots\ldots\ldots$$

Si quelques modules m_i sont identiques à quelques autres modules m_j, il faut que les solutions correspondantes soient identiques. S'il n'en est pas ainsi, le système est incompatible. De plus, tous les modules m_i étant des nombres premiers ou des puissances de nombres premiers, si l'on trouve dans le système des solutions deux modules m_i et m_j qui sont des puissances d'un même nombre premier, les solutions correspondantes sont contradictoires (dans ce cas le système est incompatible) ou sont contenues l'une dans l'autre. Dans ce dernier cas, on gardera la solution correspondant au plus grand module et l'on rejettera les autres.

Par exemple, si l'on trouve parmi les solutions

$$x \equiv 5 \pmod{8}, \qquad x \equiv 3 \pmod{8},$$

le système est incompatible.

Le système est également incompatible si l'on trouve

$$x \equiv 5 \pmod{8}, \qquad x \equiv 11 \pmod{16};$$

mais si l'on trouve

$$x \equiv 5 \pmod{8}, \qquad x \equiv 21 \pmod{32},$$

on remarquera que la solution $x \equiv 21 \pmod{32}$ est contenue dans la solution $x \equiv 5 \pmod{8}$.

On gardera la solution $x \equiv 21 \pmod{32}$ qui limite la valeur de x mieux que ne le ferait la forme $x \equiv 5 \pmod{8}$.

Ayant ainsi constaté que le système est compatible, et ayant écarté les solutions inutiles, on aura un système des solutions indépendantes :

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \quad \ldots, \quad x \equiv r_n \pmod{m_n}$$

qui donnent

$$x \equiv r \qquad (\text{mod } m = m_1, m_2, \ldots, m_n).$$

Exemples. — 1° Le système

$$13x \equiv 15 \pmod{24}, \qquad 17x \equiv 10 \pmod{25}, \qquad 17x \equiv 12 \pmod{72}$$

donne

$$5x \equiv 7 \pmod{8}, \qquad 17x \equiv 10 \pmod{25}, \qquad x \equiv 4 \pmod{8},$$
$$x \equiv 0 \pmod{3}, \qquad 8x \equiv 3 \pmod{9}.$$

La congruence $5x \equiv 7 \pmod{8}$ donne $x \equiv 3 \pmod{8}$, ce qui est incompatible avec $x \equiv 4 \pmod{8}$, dont le système est incompatible.

2° Le système

$$17x \equiv 44 \pmod{72}, \qquad 8x \equiv -1 \pmod{9}, \qquad 11x \equiv 12 \pmod{16},$$
$$100x \equiv -1 \pmod{73}$$

donne

$$x \equiv 4 \pmod{8}, \qquad 8x \equiv 8 \pmod{9}, \qquad 11x \equiv 12 \pmod{16},$$
$$100x \equiv -1 \pmod{73}, \qquad 8x \equiv 8 \pmod{9},$$

ou

$$x \equiv 4 \pmod{8}, \qquad x \equiv 1 \pmod{9}, \qquad x \equiv 4 \pmod{16},$$
$$x \equiv 27 \pmod{73}, \qquad x \equiv 1 \pmod{9}.$$

Les solutions $x \equiv 4 \pmod{8}$ et $x \equiv 4 \pmod{16}$ peuvent être remplacées par une seule : $x \equiv 4 \pmod{16}$.

On obtient ainsi les solutions indépendantes

$$x \equiv 4 \pmod{16}, \qquad x \equiv 1 \pmod{9}, \qquad x \equiv 27 \pmod{73}$$

qui donnent

$$x \equiv 100 \pmod{10512 = 16.9.73} \qquad \text{(III, 13)}.$$

3° Le système

$$11x \equiv 53 \pmod{72}, \qquad 3x \equiv 13 \pmod{100}, \qquad 679x \equiv 484 \pmod{675},$$
$$7x \equiv 25 \pmod{96}, \qquad 7x \equiv 247 \pmod{250}, \qquad 8x \equiv 68 \pmod{1125},$$
$$5x \equiv 11 \pmod{108}, \qquad 11x \equiv 21 \pmod{80}, \qquad 11x \equiv 251 \pmod{270}$$

donne successivement :

A. Module 2^m :

$$3x \equiv 5 \pmod{8}, \qquad 3x \equiv 1 \pmod{4}, \qquad 7x \equiv 25 \pmod{32},$$
$$x \equiv 1 \pmod{2}, \qquad x \equiv 3 \pmod{4}, \qquad 11x \equiv 5 \pmod{16},$$
$$x \equiv 1 \pmod{2},$$

dont les solutions sont :

$$x \equiv 7 \pmod{8}, \quad x \equiv 3 \pmod{4}, \quad x \equiv 31 \pmod{32},$$
$$x \equiv 1 \pmod{2}, \quad x \equiv 3 \pmod{4}, \quad x \equiv 15 \pmod{16},$$
$$x \equiv 1 \pmod{2}$$

et dont on gardera la solution

$$x \equiv 31 \pmod{32}.$$

B. Module 3^n :

$$2x \equiv 8 \pmod{9}, \quad 4x \equiv 25 \pmod{27}, \quad x \equiv 1 \pmod{3},$$
$$8x \equiv 5 \pmod{9}, \quad 5x \equiv 11 \pmod{27}, \quad 11x \equiv 8 \pmod{27},$$

dont les solutions sont :

$$x \equiv 4 \pmod{9}, \quad x \equiv 13 \pmod{27}, \quad x \equiv 1 \pmod{3},$$
$$x \equiv 4 \pmod{9}, \quad x \equiv 13 \pmod{27}, \quad x \equiv 13 \pmod{27}$$

et dont on gardera la solution

$$x \equiv 13 \pmod{27}.$$

C. Module 5^n :

$$3x \equiv 13 \pmod{25}, \quad 4x \equiv 9 \pmod{25}, \quad 7x \equiv 122 \pmod{125},$$
$$8x \equiv 68 \pmod{125}, \quad x \equiv 1 \pmod{5}, \quad x \equiv 1 \pmod{5},$$

dont les solutions sont :

$$x \equiv 21 \pmod{25}, \quad x \equiv 21 \pmod{25}, \quad x \equiv 71 \pmod{125},$$
$$x \equiv 71 \pmod{125}, \quad x \equiv 1 \pmod{5}, \quad x \equiv 1 \pmod{5}$$

et dont on gardera la solution

$$x \equiv 71 \pmod{125}.$$

Les modules des congruences données ne contenant pas d'autres facteurs simples que 2, 3 et 5, on peut satisfaire à toutes les congruences données avec les congruences

$$x \equiv 31 \pmod{32}, \quad \equiv 13 \pmod{27}, \quad \equiv 71 \pmod{125}$$

qui (III, 13) donnent

$$x \equiv 23071 \pmod{108000}.$$

16. Ainsi que nous l'avons vu par ce qui précède, la résolution

d'un système quelconque se ramène à un système tel que

$$x \equiv r_1 \pmod{a_1}, \quad \equiv r_2 \pmod{a_2}, \quad \ldots, \quad \equiv r_n \pmod{a_n},$$

les modules étant des nombres premiers ou des puissances de nombres premiers.

Il est facile de démontrer que ce système est toujours compatible, si les modules sont premiers entre eux.

En effet, si a_1 et a_2 sont premiers entre eux, les congruences

$$x \equiv r_1 \pmod{a_1}, \quad \equiv r_2 \pmod{a_2}$$

peuvent être remplacées par la congruence

$$a_1 y + r_1 \equiv r_2 \pmod{a_2},$$

qui est toujours possible (II, 9).

Pour ce qui est de la résolution de ce système, nous avons vu (II, 13) une solution directe très simple. Voici une autre solution.

Soit le système

$$x \equiv r_1 \pmod{a_1}, \quad \equiv r_2 \pmod{a_2}, \quad \ldots, \quad \equiv r_n \pmod{a_n}.$$

On déterminera n nombres $m_i (i = 1, 2, 3, \ldots, n)$ tels que

$$m_i \equiv 1 \pmod{a_i} \quad \text{et} \quad \equiv 0 \pmod{a_1\, a_2\, a_3 \ldots, a_{i-1}\, a_{i+1} \ldots a_n},$$

alors

$$x \equiv \sum_1^n m_i r_i \pmod{a_1\, a_2\, a_3 \ldots a_n}$$

est la solution du système donné.

En effet,

$$x \equiv \sum_1^n m_i r_i,$$

$$\equiv m_1 r_1 + m_2 r_2 + m_3 r_3 + \ldots + m_n r_n \pmod{a_1\, a_2 \ldots a_n}$$

donne

$$x \equiv m_1 r_1 \pmod{a_1},$$

car tous les termes, sauf le premier, sont divisibles par a_1 et,

puisque $m_1 \equiv 1 \pmod{a_1}$, on aura

$$x \equiv r_1 \pmod{a_1}.$$

On trouvera de même

$$x \equiv r_2 \pmod{a_2}, \qquad x \equiv r_3 \pmod{a_3}, \qquad \ldots.$$

Pour ce qui est de la détermination de n nombres m_i, le travail peut être facilité par les considérations suivantes :

Désignons par A les produits $a_1, a_2, a_3, \ldots, a_n$; le nombre

$$m_i (i = 1, 2, 3, \ldots, n)$$

est alors déterminé par les considérations suivantes :

$$m_i \equiv 1 \pmod{a_i}, \qquad \equiv 0 \left(\operatorname{mod} \frac{A}{a_i}\right);$$

donc $m_i (i = 1, 2, 3, \ldots, n)$ figure parmi les nombres

$$\frac{A}{a_i}, \quad \frac{2A}{a_i}, \quad \frac{3A}{a_i}, \quad \ldots, \quad \frac{(a_i - 1)A}{a_i}.$$

Exemples. — 1° Nous avons trouvé dans le paragraphe précédent (exemple 2°) les congruences

$$x \equiv 4 \pmod{16}, \qquad \equiv 1 \pmod{9}, \qquad \equiv 27 \pmod{73}.$$

On trouvera

$$m_1 \equiv 9.73 \equiv 657, \qquad m_2 \equiv 4.16.73 \equiv 4672,$$
$$m_3 \equiv 36.16.9 \equiv 5184 \pmod{16.9.73};$$

d'où

$$x \equiv 657.4 + 4672.1 + 5184.27 \pmod{16.9.73}$$

ou

$$x \equiv 147268 \equiv 100 \pmod{10512}.$$

2° De même la solution du troisième exemple du même paragraphe,

$$x \equiv 31 \pmod{32}, \qquad \equiv 13 \pmod{27}, \qquad \equiv 71 \pmod{225},$$

donne

$$m_1 \equiv 15.27.125 \equiv 50625, \qquad m_2 \equiv 7.32.125 \equiv 28000,$$
$$m_3 \equiv 34.32.27 \equiv 29376 \pmod{32.27.125};$$

d'où

$$x \equiv 50625.31 + 28000.13 + 29376.71 \equiv 4019071 \equiv 23071 \pmod{108000}.$$

17. Il arrive très fréquemment qu'on ait plusieurs solutions pour chaque module.

Si l'on a plusieurs congruences analogues, on aura plusieurs solutions.

Ainsi supposons que la solution conduise aux résultats suivants :

$$x \equiv r_1 \text{ ou } r_2 \text{ ou } r_3 \ldots\ldots\ldots\ldots\ldots\ldots\ r_m \quad (\text{mod } a_1),$$
$$x \equiv p_1 \text{ ou } p_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ p_n \quad (\text{mod } a_2),$$
$$x \equiv s_1 \text{ ou } s_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ s_p \quad (\text{mod } a_3),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$x \equiv t_1 \text{ ou } t_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ t_q \quad (\text{mod } a_i).$$

En combinant chacune des solutions possibles pour chaque module avec chacune des solutions possibles pour les autres modules, on obtiendra :

$$m\ n\ p\ \ldots\ q \text{ solutions } \quad (\text{mod } a_1\ a_2\ \ldots\ a_i).$$

Exemple. — Soient les deux congruences

$$x \equiv 0,\ 1,\ 4 \qquad (\text{mod } 5),$$
$$x \equiv 0,\ 4,\ 5,\ 8 \qquad (\text{mod } 16).$$

On a 3 solutions (mod 5) et 4 solutions (mod 16), ce qui équivaut à

$$3 \times 4 = 12 \text{ solutions} \qquad (\text{mod } 5.16 = 80).$$

Voici ces 12 solutions :

$$x \equiv 0.4.5.16.20.21.24.36.40.56.64.69 \qquad (\text{mod } 80).$$

Pour trouver ces 12 solutions, on peut opérer de la façon suivante : on écrira les 4 solutions (mod 16) sous la forme de

$$5.4 = 20 \text{ solutions} \qquad (\text{mod } 16.5 = 80).$$

$x \equiv$	0	4	5	8	
	16	20	21	24	
	32	36	37	40	
	48	52	53	56	
	64	68	69	72	(mod 80).

On éliminera de ce tableau les solutions $x \equiv 2.3$ (mod 5) qui ne

sont pas conformes avec la première condition $x \equiv 0.1.4 \pmod 5$. Les solutions qui doivent être éliminées sont soulignées.

Les solutions non soulignées sont celles qui répondent à la question, c'est-à-dire celles qui satisfont aux conditions imposées.

On arrive au même but par le procédé graphique suivant : On construira une table à double entrée, composée de 4 colonnes (pour les 4 solutions module 16) et de 5 lignes (le module de l'autre congruence étant 5). Les colonnes seront marquées par les nombres 0.4.5.8 (solutions module 16) et les lignes par les nombres

$$0, \quad 1 \times 16 = 16, \quad 2 \times 16 = 32, \quad 3 \times 16 = 48 \quad \text{et} \quad 4 \times 16 = 64.$$

	0.	4.	5.	8.
0.				–
16.				
32.	–	A	–	
48.	–	–	–	
64.		–		–

	0
	1
–	2
–	3
	4

–

–

De cette façon chaque case est réservée à un nombre parfaitement déterminé par la somme de deux autres, dont l'un est inscrit au début de la ligne de cette case et l'autre dans l'en-tête de la colonne de ladite case.

Ainsi la case A correspond au nombre $32 + 4 = 36$.

Cela étant, construisons une bande auxiliaire sur laquelle on écrira les nombres

$$0, \quad 16 \equiv 1, \quad 2 \times 16 \equiv 2, \quad 3 \times 16 \equiv 3 \quad \text{et} \quad 4 \times 16 \equiv 4 \pmod 5$$

avec un trait en face de 2 et 3, puisque $x \equiv 2$ ou $3 \pmod 5$ est en contradiction avec la condition

$$x \equiv 0.1 \text{ ou } 4 \pmod 5.$$

Si maintenant on applique cette bande auxiliaire le long d'une colonne, de façon que la première case de cette colonne vienne

coïncider avec le résidu (mod 5) du nombre de l'en-tête de cette colonne, toute autre case coïncidera avec le résidu (mod 5) du nombre correspondant à cette case. Il suffira, dès lors, de transférer les traits de la bande sur les cases qui viennent coïncider avec ce trait, pour éliminer les nombres qui ne conviennent pas. Les nombres restants (qui correspondent donc aux cases exemptes de trait) donnent les solutions.

On obtient ainsi les mêmes solutions que précédemment.

18. Étant donnée l'importance de cette question, nous croyons utile de résoudre encore quelques questions par le procédé graphique envisagé.

Soit, par exemple, à résoudre les congruences

$$x \equiv 1, 2 \text{ ou } 5 \pmod 7,$$
$$x \equiv 0.2.3.5 \text{ ou } 8 \pmod{11},$$
$$x \equiv 0.1.4.5.9 \text{ ou } 11 \pmod{13}.$$

Le premier tableau portera en tête des colonnes les nombres $x \equiv 0.2.3.5.8 \pmod{11}$ et sera composé de 5 colonnes et 7 lignes, ces dernières étant marquées par les nombres 0.11.22.33.44.55 et 66. Ce tableau donnera $3 \times 5 = 15$ solutions ($\text{mod } 7 \times 11 = 77$) :

	0.	2.	3.	5.	8.
0....................	–		–		
11....................	–	–	–		
22....................		–	–	–	
33....................		–		–	–
44....................		–		–	–
55....................	–			–	–
66....................	–		–		–

–	0
–	4
	1
	5
	2
–	6
	3
–	
–	

La bande sera formée de la façon suivante :

On écrira le long de la bande les nombres

$$0, \quad 11 \equiv 4, \quad 2 \times 11 \equiv 1, \quad 3 \times 11 \equiv 5, \quad 4 \times 11 \equiv 2,$$
$$5 \times 11 \equiv 6, \quad 6 \times 11 \equiv 3 \pmod 7$$

avec un trait en face de 0.3.4 et 6, solutions qui seraient en contradiction avec les solutions imposées $x \equiv 1.2.5 \pmod 7$.

Cette bande auxiliaire sera promenée le long de chaque colonne, de façon que la première case de cette colonne vienne coïncider avec le résidu du nombre de l'en-tête de la colonne (mod 7). On marquera d'un signe quelconque, par exemple d'un trait, les cases qui viennent en face d'un trait de la bande et qui correspondent aux nombres qui ne conviennent pas (mod 7).

Seules les cases exemptes d'un trait correspondent aux solutions. On obtient ainsi les 15 solutions suivantes en remplacement des 3 solutions (mod 7) et des 5 solutions (mod 11) :

$$x \equiv 2.5.8.16.19.22.30.33.36.44.47.57.58.68.71 \pmod{77}.$$

On construira un second tableau comportant 15 colonnes [pour les 15 solutions (module 77)] et 13 lignes.

Les colonnes porteront en en-têtes les 15 solutions (mod 77) et les lignes seront réservées aux nombres 0, 77, $2 \times 77 = 154$, $3 \times 77 = 231$ jusqu'à $12 \times 77 = 924$.

	2.	5.	8.	16.	19.	22.	30.	33.	36.	44.	47.	57.	58.	68.	71.
0.....	–		–	–	–			–	–		–		–	–	–
77.....			–	–		–	–	–			–			–	
154.....		–	–			–	–		–	–	–	–			
231.....	–	–			–	–			–	–		–	–		–
308.....				–	–			–	–				–	–	–
385.....	–		–				–	–			–				
462.....		–	–	–		–				–	–	–		–	
539.....	–				–	–	–		–				–		–
616.....	–	–		–				–	–	–		–		–	
693.....	–		–	–	–		–				–		–	–	–
770.....		–		–		–	–	–		–		–		–	
847.....		–	–		–		–		–	–	–	–	–		–
924.....	–	–			–	–		–		–		–	–		–

	0.
–	12
	11
–	10
	9
–	8
–	7
–	6
	5
	4
–	3
	2
	1
	0
–	
–	
–	
–	
–	

La bande sera formée des nombres

$$0, \qquad 77 \equiv 12, \qquad 2 \times 77 \equiv 11, \qquad \ldots \qquad (\text{mod } 13)$$

avec un trait en face de 2.3.6.7.8.10.12, solutions qui ne correspondent pas à celles exigées (mod 13).

On promènera cette bande le long de toutes les colonnes comme précédemment, et l'on marquera d'un trait les cases qui viennent en face d'un trait de la bande et qui correspondent aux solutions non admissibles (mod 13). Seules les cases exemptes d'un trait, correspondent à une solution. On obtient :

X ≡ 5.22.30.44.57.79.82.96.113.121.134.135.148.156.170.173.187.212.
222.225.239.247.261.264.278.299.310.313.316.330.338.352.355.365.
390.401.404.407.421.429.442.443.453.456.464.481.492.495.498.520.
533.544.547.555.572.583.586.596 607.624.635.638.646.663.674.687.
698.715.726.729.737.750.772.778.789.806.817.828.841.849.863.869.
880.915.932.940.954.960.971.992 (mod 1001).

19. Soit à trouver tous les nombres premiers avec

$$N \equiv 2.3.5 = 30, \qquad N \equiv 2.3.5.7 = 210, \qquad N \equiv 2.3.5.7.11 = 2310,$$
$$N \equiv 2.3.5.7.11.13 = 30030.$$

Les nombres premiers avec 2 sont 1 (mod 2) ou 1.3.6 (mod 6); donc les nombres premiers avec 2.3 sont 1.5 (mod 6) ou

$$1.5.7.11.13.17.19.23.25.29 \quad (\text{mod } 30).$$

Si l'on élimine de ces nombres les nombres 5 et 25 non premiers avec 5, on aura les $\varphi(30) = 8$ nombres premiers avec $2.3.5 = 30$:

$$x \equiv 1.7.11.13.17.19.23.29 \quad (\text{mod } 30).$$

Si on les développe par un tableau contenant 8 colonnes et 7 lignes, et qu'on élimine les nombres qui ne sont pas premiers avec 7 (il y aura un nombre à éliminer dans chaque colonne); on aura les $\varphi(210) = 48$ nombres qui sont premiers avec

$$210 = 2.3.5.7.$$

donc non divisibles ni par 2, ni par 3, ni par 5, ni par 7. Ce sont les nombres :

$$\begin{aligned} x \equiv\ & 1.11.13.17.19.23.29.31.37.41.43.47.53.59.61.67.71.73.79.\\ & 83.89.97.101.103.107.109.113.121.127.131.137.139.143.149.\\ & 151.157.163.167.169.173.179.181.187.191.193.197.199 \text{ et}\\ & 209 \quad (\text{mod } 210). \end{aligned}$$

Ce sont les nombres qui servent d'en-têtes dans les Tables de Lehmer (II, 3).

On obtient de même :

$$\begin{aligned} \varphi(2310) &= 480 \text{ nombres premiers avec } 2310,\\ \varphi(30030) &= 5760 \quad \text{»} \quad 30030. \end{aligned}$$

20. Soit à trouver tous les nombres inférieurs à une limite donnée et satisfaisant à plusieurs congruences données.

Pour fixer les idées, déterminons tous les nombres inférieurs à 1 000 000 et satisfaisant aux congruences :

$$\begin{aligned} x \equiv 2 \ (\text{mod } 4), \quad &\equiv \pm 1 \ (\text{mod } 9), \quad \equiv +11 \ (\text{mod } 25),\\ \equiv 0.1.2 \ (\text{mod } 7); \quad &\equiv 3.4.6.8.9 \ (\text{mod } 11),\\ \equiv 0.1.2.3.8.9.11 \ (\text{mod } 13), \quad &\equiv \pm(1.2.5.7) \ (\text{mod } 17),\\ \equiv \pm(3.5.7.8.9) \ (\text{mod } 19), \quad &\equiv \pm(0.1.2.3.4.8) \ (\text{mod } 23),\\ &\equiv \pm(0.1.4.6.8.10.11.12) \ (\text{mod } 29),\\ &\equiv \pm(3.5.8.9.10.12.13.14) \ (\text{mod } 31),\\ &\equiv \pm(1.2.4.5.6.8.10.15.17) \ (\text{mod } 37). \end{aligned}$$

On obtient successivement :

$$x \equiv 3 \ (\text{mod } 4), \qquad \equiv \pm 1 \ (\text{mod } 9),$$

ou

$$x \equiv \pm 10 \pmod{46}, \qquad x \equiv \pm 10 \pmod{36}, \qquad \equiv +11 \pmod{25},$$

ou

$$x \equiv +386.586 \pmod{900}, \qquad x \equiv 386.586 \pmod{900},$$

$$\equiv 0.1.2 \pmod{7},$$

ou, par le procédé graphique envisagé plus haut,

$$x \equiv 586.1486.2186.4186.4886.5986 \pmod{6300}.$$

Ces solutions avec celles qui sont exigées (mod 11) donnent :

$$x \equiv 2186.4186.6686.7786.10486.12986.14086.19286.20386.23086.$$
$$23786.24886.31886.32986.33686.36386.37486.42686.43786.$$
$$46286.48986.50086.52586.54586.58886.61586.62686.63386.$$
$$64486.67186 \pmod{69300}.$$

Ces solutions sont obtenues par un tableau comprenant 6 colonnes (pour les solutions correspondant au module 6300) et 11 lignes (pour les nombres 0, 6300, 2×6300, ..., 10×6300).

Mais il serait assez compliqué de continuer de cette façon. Aussi, sans chercher les formules générales des solutions pour les modules plus compliqués, écrivons tous les nombres inférieurs à 1 000 000 et satisfaisant aux solutions (mod 69300) :

0
– 10
– 7
– 4
1
11
8
– 5
2
12
9
– 6
3
–
–
–
–

On les écrira encore sous la forme d'un tableau comprenant 30 colonnes (pour les 30 solutions, mod 69300) et 15 lignes, car la seizième ligne correspondrait aux nombres supérieurs à 1 000 000.

Ainsi, la première colonne correspond aux nombres

	$69300K + 2186$	avec	$K \equiv 0.1.2\ldots14$
la deuxième	$69300K + 4186$	avec	$K \equiv 0.1.2\ldots14$
la troisième	$69300K + 6686$	avec	$K \equiv 0.1.2\ldots14$
la treizième	$69300K + 31886$	avec	$K \equiv 0.1.2\ldots13$
la trentième	$69300K + 67186$	avec	$K \equiv 0.1.2\ldots13$

Le tableau ne contiendra donc que

$$12.15 + 18.14 = 432$$

nombres inférieurs à 1 000 000 et satisfaisant aux formes exigées par le module 69300.

On construira une bande auxiliaire qui portera sur sa longueur les nombres

$$0, \quad 69300 \equiv 10, \quad 2 \times 69300 \equiv 7, \quad 3 \times 69300 \equiv 4, \quad \ldots \quad (\text{mod } 13)$$

avec un trait en face des nombres 4.5.6.7.10.12 qui ne conviennent pas (mod 13).

On promènera cette bande le long de toutes les colonnes, de façon que la première case de chaque colonne coïncide avec le résidu (mod 13) du nombre de l'en-tête de la colonne.

Alors chaque case viendra coïncider avec le résidu (mod 13) du nombre qui correspond à cette case. On marquera un trait (ou le nombre 13) dans les cases qui viennent en face d'un trait. Seules les cases exemptes d'un trait (ou du nombre 13) satisfont à toutes les conditions exigées par les modules 69300 et 13.

Il ne reste que 230 nombres satisfaisant à ces conditions (230 cases exemptes d'un trait ou du nombre 13).

On éliminera ceux de ces 230 nombres qui ne sont pas

$$\equiv \pm 1.2.5.7 \quad (\text{mod } 17)$$

ou qui sont

$$\equiv 0.3.4.6.8.9.11.13.14 \quad (\text{mod } 17)$$

au moyen d'une autre bande portant sur sa longueur les nombres

$$0, \quad 69300 \equiv 8, \quad 2 \times 69300 \equiv 16, \quad 3 \times 69300 \equiv 7, \quad \ldots$$

avec un trait en face de

$$0.3.4.6.8.9.11.13.14.$$

On promènera cette bande comme précédemment et l'on marquera d'un signe quelconque (ou le nombre 17) dans les cases qui viennent en face d'un trait.

Il ne reste que 102 cases exemptes d'un trait ou du nombre 17, qui correspondent aux 102 nombres inférieurs à 1 000 000 et qui satisfont à toutes les conditions imposées par les modules 69 300, 13 et 17.

Au moyen d'une bande portant sur sa longueur les nombres

$$0, \quad 69\,300 \equiv 7, \quad 2 \times 69\,300 \equiv 14, \quad 3 \times 69\,300 \equiv 2, \quad \ldots \quad (\bmod 19)$$

et un trait en face de

$$0.1.2.4.6.13.15.17.18;$$

on éliminera les nombres ne convenant pas (mod 19).

Il ne restera que 55 nombres dont le plus petit est 58 886 et le plus grand 953 486 qui satisfont à toutes les conditions exigées par les modules 69 300, 13, 17 et 19.

De la même façon, on éliminera les nombres ne convenant pas pour le module 23.

Après cette opération, il ne reste que les 25 nombres suivants :

$$x \equiv 132\,686.181\,286.182\,386.227\,186.230\,986.287\,686.314\,686.327\,286.$$
$$339\,886.409\,886.453\,286.491\,786.508\,186.549\,586.667\,486.682\,586.$$
$$700\,786.705\,986.812\,386.823\,886.863\,486.881\,686.886\,186.921\,286$$
$$\text{et } 953\,486$$

qui satisfont à toutes les conditions envisagées jusqu'ici.

Si l'on élimine les nombres ne convenant pas (mod 29), il reste

$$x \equiv 132\,686.227\,186.230\,986.287\,686.327\,286.339\,886.409\,886.491\,786.$$
$$508\,186.700\,786.705\,986.823\,886.863\,486.881\,686.886\,186,$$

dont les six suivants satisfont aux conditions imposées par le module 31 :

$$x \equiv 227\,186.230\,986.327\,286.508\,186.705\,986.863\,486.$$

De ces six nombres, seuls les trois suivants :

$$x \equiv 227\,186.230\,986.863\,486,$$

satisfont aux conditions imposées par le module 37, ainsi qu'à toutes les conditions exigées par tous les autres modules.

21. Il est facile d'imaginer une machine à laquelle on pourrait confier l'élimination des solutions qui ne conviennent pas pour un module quelconque.

Supposons qu'on fasse le tableau précédemment étudié (III, 17, 20) de sorte qu'il ne soit composé que d'une seule colonne, mais d'un nombre de lignes suffisamment grand. Les bandes aussi seront d'une longueur suffisante. Si l'on pose les bandes correspondant aux différents modules les unes à côté des autres, de façon que le nombre de la première ligne coïncide avec le résidu du nombre de l'en-tête de la colonne, une solution sera donnée par une ligne blanche à travers toutes les bandes.

Une bande de longueur indéfinie peut être réalisée par une circonférence tournant autour de son centre.

Imaginons un système d'engrenages composé d'un certain nombre de paires de roues montées sur deux axes parallèles, A et A'.

Les roues montées sur l'axe A ont toutes le même nombre de dents, par exemple 64, et sont solidaires avec l'axe. Les roues qui leur correspondent sur l'autre axe A' sont folles sur l'axe et ont un nombre variable de dents.

Ainsi, si l'on désigne par n_1 et n_2 le nombre de dents, et par R_1 et R_2 les rayons, on peut prendre une distance entre les axes A et A' de 200^{mm} et les valeurs suivantes de n_1, n_2, R_1, R_2 (en millimètres) :

	n_1.	n_2.	R_1.	R_2.
Pour le module 2^n	64	64	100	100
» 3 ou 9 ou 27	64	54	108.7	91.3
» 5 ou 25	64	50	109.3	90.7
» 7 ou 49	64	49	110.3	89.7
» 11	64	44	118.5	81.5
» 13	64	52	111.3	88.7
» 17	64	51	112.3	87.7
» 19	64	57	106.0	94.0
» 23	64	46	116.3	83.7
» 29	64	58	105.9	95.0
» 31	64	62	100.9	99.1
» 37	64	37	126.8	73.2
» 41	64	41	122.0	78.0
» 43	64	43	119.6	80.4
» 47	64	47	115.3	84.7

Sur les roues montées sur l'axe A', on tracera une circonférence d'un rayon inférieur à la plus petite valeur de R_2, par exemple d'un rayon de 65^{mm}.

Cette circonférence sera divisée en n_2 parties égales. Aux points de division, on percera des trous, ou bien on placera un contact électrique, suivant qu'on se propose de se servir d'un rayon de lumière ou de courant électrique. Ces trous ou contacts seront numérotés.

Cela étant, si l'on a un système de congruences dont les modules sont inférieurs à 50, on procédera de la façon suivante : On bouchera les trous qui correspondent aux numéros n_1 qui sont des solutions non admissibles (mod p). Si l'on se sert de contacts électriques, on enlèvera les contacts des numéros qui correspondent aux solutions non admissibles.

La machine étant mise en marche, quand elle présentera une série de trous non bouchés, ou une série de contacts alignés, donnera un nombre satisfaisant à toutes les conditions imposées. Ce phénomène sera constaté par un rayon lumineux faisant tache sur un écran placé devant la machine si l'on se sert de trous perforés. Si l'on se sert de contacts électriques, on s'arrangera de façon que, par une série de contacts alignés, la machine soit arrêtée. Dans les deux cas, on sera extérieurement informé de ce qu'une solution est obtenue. Un compte-tours placé sur l'axe A donnera le nombre de tours effectués et, partant, la solution.

22. Considérons un système de n congruences de même module à n inconnues :

$$
\begin{aligned}
&a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \ldots + a_{1k}x_k \ldots + a_{1n}x_n \equiv b_1 \qquad (\text{mod } m),\\
&a_{21}x_1 \ldots\ldots\ldots\ldots\ldots + a_{2k}x_k \ldots\ldots\ldots\ldots \equiv b_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&a_{n1}x_1 + a_{r2}x_2 \ldots\ldots\ldots + a_{nk}x_k \ldots\ldots\ldots\ldots \equiv b_n.
\end{aligned}
$$

Si l'on forme le tableau rectangulaire

$$
\left\|
\begin{array}{l}
a_{11}\ a_{12}\ a_{13} \ldots a_{1k} \ldots a_{1n} - b_1\\
a_{21}\ a_{22}\ a_{23} \ldots a_{2k} \ldots a_{2n} - b_2\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_{n1}\ a_{n2}\ a_{n3} \ldots a_{nk} \ldots a_{nn} - b_n
\end{array}
\right\|
$$

composé de n lignes et de $(n+1)$ colonnes, et si l'on désigne par $D_1, D_2, D_3, \ldots, D_n$, D les déterminants qu'on obtient du tableau rectangulaire, en supprimant dans ce tableau la première, deuxième, troisième, ..., $n^{\text{ième}}$ dernière colonne, on aurait

$$\frac{-x_1}{D_1} = \frac{x_2}{D_2} = \frac{-x_3}{D_3} = \ldots = \frac{(-1)^n x_n}{D_n} = \frac{(-1)^{n+1}}{D}$$

si le système donné était un système d'équation.

Il est évident qu'en remplaçant la solution précédente par

$$\frac{-x_1}{D_1} \equiv \frac{x_2}{D_2} \equiv \frac{-x_3}{D_3} \equiv \ldots \equiv \frac{(-1)^n x_n}{D_n} \equiv \frac{(-1)^{n+1}}{D} \pmod{m},$$

on aura la solution du système de congruences.

Cette solution peut être achevée de la manière suivante : On a

$$x_i \equiv \pm \frac{D_i}{D} \pmod{m}$$

ou

$$D x_i \equiv \pm D_i \pmod{m};$$

d'ailleurs, nous pouvons (II, **11**) interpréter la solution

$$x_i \equiv \pm \frac{D_i}{D} \pmod{m}.$$

Exemple. — Soit le système

$$\begin{aligned} 2x - 3y - 5z &\equiv 7 \pmod{101}, \\ 3x - 6y - 8z &\equiv 11, \\ 8x + y + 2z &\equiv 2, \end{aligned}$$

Le tableau rectangulaire

$$\left\| \begin{matrix} 2 & -3 & -5 & -7 \\ 3 & -6 & -8 & -11 \\ 8 & +1 & +2 & -2 \end{matrix} \right\|$$

donne

$$D_1 = +29, \qquad D_2 = -4, \qquad D_3 = -65, \qquad D_4 = -53;$$

d'où

$$\frac{-x}{29} \equiv \frac{y}{-4} \equiv \frac{-z}{-65} \equiv \frac{+1}{-53} \pmod{101};$$

$$53x \equiv 29 \quad \text{donne} \quad x \equiv 52 \pmod{101},$$
$$53y \equiv 4 \quad \text{»} \quad y \equiv 42,$$
$$53z \equiv -65 \quad \text{»} \quad z \equiv 75.$$

CHAPITRE III.

GÉNÉRALITÉS SUR LES CONGRUENCES DE DEGRÉS SUPÉRIEURS.

1. Théorème de Fermat. — *Si p est un nombre premier et a non divisible par p, on aura*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Considérons les deux termes de la progression

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (p-1)a$$

et soient

$$r_1, \quad r_2, \quad r_3, \quad \ldots, \quad r_{p-1}$$

leurs résidus (mod p), de sorte que

$$a \equiv r_1, \quad 2a \equiv r_2, \quad 3a \equiv r_3, \quad \ldots, \quad (p-1)a \equiv r_{p-1} \pmod{p}.$$

Si l'on fait le produit de ces congruences, membre à membre, il vient

$$1.2.3.4\ldots(p-1)a^{p-1} \equiv r_1 r_2 r_3 \ldots r_{p-1} \pmod{p}.$$

Or, les facteurs r_1, r_2, r_3, ..., r_{p-1} ne diffèrent que par l'ordre des facteurs 1, 2, 3, 4, ... $(p-1)$ (I, 9); donc

$$r_1 r_2 r_3 \ldots r_{p-1} = 1.2.3\ldots(p-1).$$

En supprimant de la dernière congruence les facteurs communs

$$1.2.3.4\ldots(p-1) \doteq r_1 r_2 r_3 \ldots r_{p-1},$$

il vient

$$a^{p-1} \equiv 1 \pmod{p}.$$

Remarque. — Quel que soit a, on aura $a^p \equiv a \pmod{p}$ si p est premier.

En effet, la congruence $a^p \equiv a \pmod{p}$ est vraie non seulement quand a n'est pas divisible par p (alors $a^{p-1} \equiv 1$ et $a^p \equiv a$), mais aussi quand a est un multiple de p.

2. Le théorème que nous venons de démontrer est d'une importance capitale dans la théorie des nombres. Aussi allons-nous donner une autre démonstration de ce théorème :

Soit donc p un nombre premier et a non divisible par p. On a

$$(a+b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{2}a^{p-2}b^2 + \ldots + pab^{p-1} + b^p.$$

Il est facile de voir que tous les termes du second membre, sauf les termes extrêmes, sont divisibles p r p ; donc

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Si, dans cette congruence, on remplace b par $b+c$, il vient

$$(a+b+c)^p \equiv a^p + (b+c)^p \equiv a^p + b^p + c^p \pmod{p}.$$

En continuant de cette façon, on arrivera à

$$(a+b+c+\ldots+k+l)^p \equiv a^p + b^p + c^p + \ldots + k^p + l^p \pmod{p}.$$

Si l'on fait dans cette congruence

$$a = b = c = \ldots = k = 1$$

et leur nombre égal à a, on aura

$$a^p \equiv 1+1+1+\ldots+1 \equiv a \pmod{p}.$$

Si a n'est pas divisible par p, on peut supprimer le facteur commun a et écrire

$$a^{p-1} \equiv 1 \pmod{p}.$$

3. Euler est le premier qui ait démontré le théorème de Fermat. C'est encore Euler qui a donné le théorème suivant, dont celui de Fermat n'est qu'un cas particulier :

Si l'on désigne par $\varphi(\mathrm{N})$ *l'indicateur de* N (I, 15) *et si* a *est premier avec* N, *on aura*

$$a^{\varphi(\mathrm{N})} \equiv 1 \pmod{\mathrm{N}}.$$

En effet, soient

$$\mathrm{N}_1,\quad \mathrm{N}_2,\quad \mathrm{N}_3,\quad \ldots,\quad \mathrm{N}_n$$

les $n = \varphi(\mathrm{N})$ nombres inférieurs à N et premiers avec lui.

Considérons les nombres

$$aN_1, \quad aN_2, \quad aN_3, \quad \ldots, \quad aN_n$$

et soient

$$r_1, \quad r_2, \quad r_3, \quad \ldots, \quad r_n$$

leurs résidus positifs (mod N), de sorte qu'on aura

$$aN_1 \equiv r_1, \qquad aN_2 \equiv r_2, \qquad \ldots, \qquad aN_n = r_n \qquad (\text{mod } N).$$

Puisque a et N_i ($i = 1, 2, 3, \ldots, n$) sont premiers avec N, le produit aN_i est aussi premier avec N et le nombre r_i qui lui est congru est inférieur à N et premier avec lui; donc r_i figure parmi les nombres

$$N_1, \quad N_2, \quad N_3, \quad \ldots, \quad N_n.$$

D'autre part, les valeurs de r_i ($i = 1, 2, 3, \ldots, n$) sont toutes distinctes, car si l'on avait $r_i = r_k$, il en résulterait

$$aN_i \equiv aN_k \qquad (\text{mod } N)$$

ou, puisque a est premier avec N,

$$N_i \equiv N_k \qquad (\text{mod } N),$$

ce qui est impossible, étant donné que N_i et N_k sont tous deux inférieurs à N.

Il en résulte que les facteurs du produit $r_1 r_2 r_3 \ldots r_n$ ne diffèrent que par l'ordre des facteurs du produit $N_1 N_2 \ldots N_n$.

Si maintenant on fait, membre à membre, les produits des congruences

$$aN_1 \equiv r_1, \qquad aN_2 \equiv r_2, \qquad \ldots, \qquad aN_n \equiv r_n \qquad (\text{mod } N),$$

il vient

$$a^n N_1 N_2 N_3 \ldots N_n \equiv r_1 r_2 r_3 \ldots r_n \qquad (\text{mod } N)$$

et, en supprimant les facteurs communs, premiers avec le module,

$$N_1 N_2 N_3 \ldots N_n \equiv r_1 r_2 r_3 \ldots r_n,$$

on aura

$$a^n \equiv 1 \qquad (\text{mod } N)$$

ou

$$a^{\varphi(N)} \equiv 1 \qquad (\text{mod } N).$$

On notera que si N est premier, $\varphi(N) = N - 1$ et l'on aura le théorème de Fermat.

4. On peut appliquer ces deux théorèmes pour la résolution de congruences du premier degré.

Supposons d'abord que le module est premier.

Pour résoudre la congruence

$$ax \equiv b \pmod{m},$$

a étant premier avec p, remarquons qu'on a (mod m)

$$a^{p-1} \equiv 1, \quad \text{ou} \quad b a^{p-1} \equiv b, \quad \text{ou} \quad a b a^{p-2} \equiv b.$$

En comparant cette identité avec la congruence

$$ax \equiv b \pmod{m},$$

on voit qu'on peut prendre

$$x \equiv b a^{p-2} \pmod{p}.$$

Pour trouver la valeur de $x \equiv \frac{b}{a} \pmod{p}$, on peut aussi multiplier membre à membre cette congruence et la congruence $1 \equiv a^{p-1}$; il vient

$$x \equiv b a^{p-2} \pmod{p}.$$

Si, enfin, p n'est pas premier, on multipliera, membre à membre, les congruences

$$1 \equiv a^{\varphi(p)} \quad \text{et} \quad x \equiv \frac{b}{a} \pmod{p},$$

il vient

$$x \equiv b a^{\varphi(p)-1} \pmod{p}.$$

5. Théorème. — *Les diviseurs primitifs d'un nombre de la forme $a^n - 1$ sont de la forme $kn + 1$.*

Remarquons d'abord qu'on entend par diviseur primitif d'un nombre de la forme $a^n - 1$, un diviseur de $a^n - 1$ qui ne divise $a^x - 1$ pour aucune valeur de x inférieure à n.

Ainsi :

$$2^{25} - 1 = 31.601.1801.$$

De ces trois facteurs, le premier, 31, divise $2^5 - 1$ et n'est pas un diviseur primitif; les deux autres ne divisent $2^x - 1$ que pour

$$x = 25.50.75\ldots = 25\mathrm{K}$$

et la plus petite valeur de x est $x = 25$. Ces deux facteurs sont donc primitifs.

Remarquons encore que si $2^n - 1$ est divisible par p, p étant un diviseur primitif, on aura

$$a^n \equiv 1 \pmod{p},$$

et puisque, d'après le théorème de Fermat,

$$a^{p-1} \equiv 1 \pmod{p},$$

n est nécessairement un diviseur de $p - 1$, car la suite

$$a^0 = 1, \quad a^1 a^2 a^3 a^4 \ldots a^n = 1, \quad a^{n+1} \equiv a' \ldots a^{n+k} \equiv a^k, \quad a^{p-1} \equiv 1 \pmod{p}$$

renferme nécessairement un nombre entier de périodes

$$1, \quad a, \quad a^2 a^3 a^4 \ldots a^n.$$

Ainsi $p - 1$ est divisible par n. Si l'on désigne par k le quotient de $p - 1$ par n, on aura

$$p - 1 = kn \quad \text{ou} \quad p = kn + 1.$$

Nous reviendrons sur ce sujet qui est d'une importance capitale (V, **24**).

6. Nous allons nous occuper maintenant des congruences de degré supérieur dont le module sera supposé premier. La forme générale d'une telle congruence est

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + x + K \equiv 0 \pmod{p}.$$

Les coefficients A, B, C, ..., K sont des nombres positifs ou négatifs, mais entiers.

Remarquons d'abord que le coefficient du terme qui contient la puissance la plus élevée de x peut être transformé en 1 sans que les autres coefficients ne deviennent fractionnaires.

Si, en effet, a est l'associé de A (mod p) (II, **12**), on aura

$$Aa \equiv 1.$$

En multipliant par a la congruence donnée, on aura

$$x^m + Bax^{m-1} + Cax^{m-2} + \ldots + ax + Ka \equiv 0 \pmod{m}.$$

Si A est divisible par p, le nombre A n'a pas d'associé, mais alors on peut simplement supprimer le terme Ax^m qui est $\equiv 0 \pmod{p}$.

Ainsi, ayant la congruence $2x^3 + 3x + 7 \equiv 0 \pmod{11}$ et l'associée de 2 (mod 11) étant 6, multiplions la congruence donnée par 6, on aura

$$x^3 + 7x + 9 \equiv 0 \pmod{11}.$$

7. Théorème. — *Une congruence de degré m*

$$x^m + Ax^{m-1} + Bx^{m-2} + \ldots + Hx + K \equiv 0 \pmod{p}$$

n'admet pas plus de m solutions différentes.

On remarquera que si $x \equiv a \pmod{p}$ est une solution de la congruence donnée, le premier membre est divisible par

$$x - a \pmod{p}.$$

En effet, soient Q (polynome du degré $m - 1$) le quotient, et R le reste de la division de

$$x^m + Ax^{m-1} + \ldots + Hx + K \quad \text{par} \quad x - a,$$

on aura

$$x^m + Ax^{m-1} + \ldots + Hx + K \equiv (x - a)Q + R \pmod{p}.$$

Si l'on fait $x \equiv a$, on a $R \equiv 0$; donc

$$x^m + Ax^{m-1} + \ldots + Hx + K \equiv (x - a)Q \equiv (x - a)(x^{m-1} + A_1x^{m-2} + \ldots).$$

Ainsi à chaque solution $x \equiv a \pmod{p}$ correspond un facteur linéaire dans la décomposition du premier membre de la congruence.

Puisque le nombre de facteurs linéaires n'est pas supérieur à m, le nombre des solutions différentes n'est pas supérieur à m.

On énonce quelquefois ce théorème autrement en disant que la congruence

$$Ax^m + Bx^{m-1} + \ldots + Hx + K \equiv 0 \pmod{p}$$

n'admet pas plus de m solutions, à moins que tous les coefficients ne soient divisibles par p, et alors elle a une infinité de solutions.

Ou encore : si la congruence

$$Ax^m + Bx^{m-1} + \ldots + Hx + K \equiv 0 \pmod{p}$$

admet plus de m solutions, tous les coefficients sont $\equiv 0 \pmod p$.

8. Considérons l'expression

$$f(x) = (x-1)(x-2)(x-3)\ldots[x-(p-1)] - (x^{p-1}-1)$$

composée de deux termes dont le premier est le produit de $(p-1)$ facteurs $x-1$, $x-2$, ..., $x-(p-1)$ et le deuxième est $x^{p-1}-1$.

Chacun de ces deux termes s'annule pour

$$x = 1.2.3\ldots p-1.$$

Donc la congruence

$$(x) \equiv 0 \pmod p$$

admet $p-1$ solutions.

Mais $f(x)$ n'est que du degré $p-2$, car les termes x^{p-1} disparaîtront, donc tous les coefficients de $f(x)$ sont $\equiv 0 \pmod p$.

Les coefficients de $f(x)$ sont :

$1-1\equiv 0$	pour le terme en	x^{p-1},
$-(1+2+3+\ldots+p+1)$	»	x^{p-2},
$+(1.2+1.3+\ldots+2.3+\ldots)$	»	x^{p-3},
....		....,
$(-1)^{p-1}1.2.3.4\ldots(p-1)+1$	»	x^0.

On aura ainsi :

$$1+2+3+\ldots+(p-1) \equiv 0 \pmod p,$$
$$1.2+1.3+\ldots+2.3+\ldots+(p-2)(p-1) \equiv 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$(-1)^{p-1}1.2.3\ldots(p-1)+1 \equiv 0.$$

9. Théorème de Vilson. — *Si p est un nombre premier, on aura*

$$1.2.3\ldots(p-1)+1 \equiv 0 \pmod p.$$

Le théorème est vrai pour $p=2$, car $1+1\equiv 0 \pmod 2$.

Si $p>2$, p est impair et $p-1$ est pair.

La dernière relation trouvée dans le paragraphe précédent devient

$$1.2.3\ldots(p-1)+1 \equiv 0.$$

Il est à noter que le théorème de Vilson est une caractéristique de nombres premiers, mais malheureusement inapplicable pour reconnaître si un nombre est premier.

10. Théorème. — *Tout nombre premier de la forme $4n+1$ est un diviseur d'une somme de deux carrés.*

En effet, si $p = 4n+1$ est premier, on aura

$$1.2.3\ldots(4n)+1 \equiv 0 \pmod{p}$$

ou

$$1.2.3\ldots(2n)(2n+1)(2n+2)\ldots(4n)+1 \equiv 0 \pmod{p}.$$

Les $4n$ nombres formant le produit $(4n)!$ peuvent être distribués en deux groupes, chacun contenant $2n$ facteurs.

De plus, ces facteurs sont, au signe près, les mêmes $(\bmod\ p)$. Ainsi :

$$4n \equiv -1\ 4n-1 \equiv -2\ldots 2n+2 \equiv -(2n-1),\ 2n+1 \equiv -2n \pmod{p}.$$

Le nombre des facteurs de chaque groupe étant pair, le changement de signe de ces facteurs n'altère pas le résultat et l'on aura

$$[1.2.3\ldots(2n)]^2+1 \equiv 0 \pmod{p};$$

donc le nombre premier $p = 4n+1$ est un diviseur de

$$[1.2.3\ldots(2n)]^2+1$$

ou d'une somme de deux carrés.

11. Si la congruence

$$Ax^m + Bx^{m-1} + \ldots + Hx + K \equiv 0 \pmod{p}$$

admet m solutions $a_1, a_2, \ldots, a_m$, on aura

$$\begin{aligned} -A(a_1+a_2+a_3+\ldots+a_m) &\equiv B \pmod{p},\\ A(a_1a_2+a_1a_3+\ldots\ldots) &\equiv C,\\ \ldots\ldots\ldots\ldots\ldots\ldots&\ldots,\\ (-1)^m A\,a_1a_2a_3+\ldots\ldots+a_m) &\equiv K. \end{aligned}$$

En effet, on aura

$$Ax^m + Bx^{m-1}+\ldots+Hx+K \equiv A(x-a_1)(x-a_2)\ldots(x-a_m) \pmod{p}$$

ou

$$\begin{aligned} Ax^m + Bx^{m-1}+\ldots+Hx+K \equiv Ax^m &- A(a_1a_2a_3+\ldots+)x^{m-1}\\ &+ A(a_1a_2+a_1a_3\ldots)x^{m-2}+\ldots\\ &+(-1)^m A\,a_1a_2\ldots a_m \pmod{p}. \end{aligned}$$

Cette dernière congruence étant du degré $m-1$ et admettant m solutions $a_1, a_2, \ldots, a_m$ aura tous les coefficients $\equiv 0 \pmod{p}$; donc

$$\begin{aligned} -A(a_1+a_2+a_3+\ldots) &\equiv B \pmod{p},\\ +A(a_1a_2+a_1a_3+\ldots) &\equiv C,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots &,\\ (-1)^m A a_1 a_2 a_3 \ldots a_m &\equiv K. \end{aligned}$$

12. Théorème. — *Les solutions communes à deux congruences*

$$f(x) \equiv 0 \quad \text{et} \quad F(x) \equiv 0 \pmod{p}$$

sont aussi solutions de la congruence $D(x) \equiv 0 \pmod{p}$, $D(x)$ *étant le plus grand commun diviseur* $\pmod{p}$ *de* $f(x)$ *et de* $F(x)$.

En effet, à toute solution $x \equiv a \pmod{p}$ des congruences

$$f(x) \equiv 0 \quad \text{et} \quad F(x) \equiv 0 \pmod{p}$$

correspond un facteur linéaire $x-a$ dans la décomposition de $f(x)$ et $F(x)$, donc dans la décomposition de $D(x)$; par conséquent $x \equiv a \pmod{p}$ sera aussi solution de $D(x) \equiv 0 \pmod{p}$.

Inversement, les solutions de $D(x) \equiv 0 \pmod{p}$ sont aussi solutions de $f(x) \equiv 0$ et de $F(x) \equiv 0$.

13. Théorème. — *Si m est supérieur à p, la congruence du degré $m \pmod{p}$ peut être remplacée par une congruence du degré $p-1$ qu'on obtient en cherchant le reste de la division du polynome donné du degré m par $x^p - x$.*

Soit

$$Ax^m + Bx^{m-1} + \ldots + Hx + K \equiv 0 \pmod{p}$$

la congruence donnée. Divisons

$$Ax^m + Bx^{m-1} + \ldots + Hx + K \quad \text{par} \quad x^p - x$$

et soient Q (un polynome du degré $m-p$) le quotient et R le reste. R est un polynome du degré $p-1$ au plus, tel que

$$A_1x^{p-1} + B_1x^{p-2} + \ldots + H_2x + K.$$

On aura

$$\begin{aligned} \mathrm{A}x^m + \mathrm{B}x^{m-1} + \ldots + \mathrm{H}x + \mathrm{K} \equiv (x^p - x)\mathrm{Q} \\ + (\mathrm{A}_1 x^{p-1} + \mathrm{B}_1 x^{p-2} + \ldots + \mathrm{H}_1 x + \mathrm{K}) \\ (\mathrm{mod}\ p). \end{aligned}$$

Puisque $(x^p - x)\mathrm{Q}$ est $\equiv 0 \pmod p$ quel que soit x, les deux congruences

$$\mathrm{A}x^m + \mathrm{B}x^{m-1} + \ldots + \mathrm{H}x + \mathrm{K} \equiv 0 \qquad (\mathrm{mod}\ p)$$

et

$$\mathrm{A}_1 x^{p-1} + \mathrm{B}_1 x^{p-2} + \ldots + \mathrm{H}_1 x + \mathrm{K}_1 \equiv 0$$

ont les mêmes solutions, ce qui démontre le théorème.

14. Théorème. — *Si la congruence*

$$f(x) = x^m + \mathrm{A}x^{m-1} + \ldots + \mathrm{H}x + \mathrm{K} \equiv 0 \qquad (\mathrm{mod}\ p)$$

admet m solutions, tous les coefficients du reste de la division de $x^p - x$ par $f(x)$ sont $\equiv 0 \pmod p$.

Soient $\mathrm{F}(x)$ le quotient et $\mathrm{R}(x)$ le reste de la division de $x^p - x$ par $f(x)$. On aura

$$x^p - x = f(x)\,\mathrm{F}(x) + \mathrm{R}(x)$$

ou

$$x^p - x - f(x)\,\mathrm{F}(x) = \mathrm{R}(x).$$

Or le premier membre de cette égalité est $\equiv 0 \pmod p$ pour m valeurs de x, au moins, car $x^p - x$ est $\equiv 0$ pour toute valeur de x et $f(x)\mathrm{F}(x)$ est $\equiv 0 \pmod p$ pour au moins m valeurs qui satisfont $f(x) \equiv 0 \pmod p$. Donc la congruence $\mathrm{R}(x) \equiv 0 \pmod p$ admet aussi au moins m solutions. Comme $\mathrm{R}(x)$ est le reste de la division de $x^p - x$ par $f(x)$ qui est un polynome du degré m, le reste $\mathrm{R}(x)$ est d'un degré inférieur à m. Et puisque la congruence $\mathrm{R}(x) \equiv 0$ admet au moins m solutions, tout en étant d'un degré inférieur à m, tous les coefficients de cette congruence sont $\equiv 0 \pmod p$.

15. Inversement, *si dans le reste de la division de*

$$x^p - x \quad \text{par} \quad f(x) = \mathrm{A}x^{m-1} + \ldots + \mathrm{H}x + \mathrm{K},$$

tous les coefficients sont $\equiv 0 \pmod p$, *la congruence*

$$f(x) \equiv 0 \pmod p$$

admet m solutions.

Soient $F(x)$ le quotient et $R(x)$ le reste de la division de $x^p - x$ par $f(x)$; on aura

$$x^p - x = f(x)F(x) + R(x)$$

ou

$$x^p - x - R(x) = f(x)F(x).$$

Le premier membre de cette égalité est congru à $0 \pmod p$ pour toutes valeurs de x, car les deux termes qui le composent $x^p - x$ et $R(x)$ sont congrus à $0 \pmod p$ pour toute valeur de x.

Donc la congruence

$$f(x)F(x) \equiv 0 \pmod p$$

peut être satisfaite par n'importe quelle valeur de x.

Or, le quotient de la division de $x^p - x$ par $f(x)$ est du degré $p - m$ et son premier terme est x^{p-m}; conséquemment, la congruence $f(x) \equiv 0 \pmod p$ n'a pas plus de m solutions, et la congruence $F(x) \equiv 0 \pmod p$ plus de $p - m$ solutions.

Puisque la congruence $f(x)F(x) \equiv 0 \pmod p$ du degré $m + (p - m)$ admet p solutions

$$x \equiv 0.1.2.3\ldots(p-1) \pmod p,$$

il en résulte que la congruence $f(x) \equiv 0 \pmod p$ admet m solutions et la congruence $F(x) \equiv 0 \pmod p$ admet $p - m$ solutions.

Exemples. — 1° La congruence

$$x^3 + x^2 + 4x + 1 \equiv 0 \pmod 7$$

admet trois solutions, car le reste de la division de

$$x^7 - x \quad \text{par} \quad x^3 + x^2 + 4x + 1 \quad \text{est} \quad -28x^2 - 35x - 7,$$

puisque

$$x^7 - x = (x^3 + x^2 + 4x + 1)(x^4 - x^3 - 3x^2 + 6x + 7) - 7(4x^2 + 5x + 1).$$

2° La congruence

$$x^3 - x^2 + x - 1 \equiv 0 \pmod{7}$$

admet moins de trois solutions, car le reste de la division de

$$x^7 - x \quad \text{par} \quad x^3 - x^2 + x - 1 \quad \text{est} \quad x^2 - 2x + 1,$$

puisque

$$x^7 - x = (x^3 - x^2 + x - 1)(x^4 + x^3 + 1) + (x^2 - 2x + 1).$$

CHAPITRE IV.

CONGRUENCES DU SECOND DEGRÉ.

1. La forme générale d'une congruence du second degré est

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Remarquons que si $a \equiv 0 \pmod{p}$, la congruence donnée n'est que du premier degré. Nous supposons donc a différent de $0 \pmod{p}$.

Le module lui-même doit être supérieur à 2, car si $p = 2$, la congruence donnée peut être remplacée par une autre du degré $p - 1 = 2 - 1 = 1$ (III, 13).

Supposons donc $p > 2$ et pour commencer supposons p premier. Dans ces conditions, la congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

est équivalente à

$$(2ax + b)^2 = b^2 - 4ac \pmod{p}$$

ou

$$z^2 = q \pmod{p},$$

étant posé

$$2ax + b \equiv z \quad \text{et} \quad b^2 - 4ac = q.$$

Si l'on parvient à résoudre la congruence

$$z^2 \equiv q = b^2 - 4ac \pmod{p},$$

on aura, pour déterminer x, l'équation $2ax + b = z$ ou la congruence

$$2ax + b \equiv z \pmod{p}$$

que nous savons résoudre (II, 10).

Ainsi toute congruence de second degré

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

se ramène à

$$z^2 = q \pmod{p}.$$

Nous allons donc nous occuper de cette dernière.

2. Nous supposons que q n'est pas $\equiv 0 \pmod p$, car autrement la seule solution de la congruence est $z \equiv 0 \pmod p$. En effet, $z^2 \equiv 0 \pmod p$ exprime la divisibilité de z^2 par p. Or, p étant premier, z^2 n'est divisible par p que si z l'est; donc $z \equiv 0 \pmod p$ est la seule solution possible de la congruence $z^2 \equiv 0 \pmod p$.

Nous allons prouver que si $q \not\equiv 0 \pmod p$, la congruence $z^2 \equiv q \pmod p$ admet deux solutions ou n'en admet aucune.

On sait que la congruence $z^2 \equiv q \pmod p$ a autant de solutions qu'il y a de nombres dans la suite $0, 1, 2, 3, \ldots, p-1$, qui lui satisfont. D'autre part, cette congruence ne peut pas avoir plus de deux solutions.

A cause de $a^2 \equiv (p-a)^2$, on voit qu'à toute solution $z = a$ correspond une solution $z = p - a$ distincte de la première, puisque $a = p - a$ entraînerait $p = 2a$; or p est premier par hypothèse. D'autre part, si $a < p - 1$, $p - a$ est aussi $< p - 1$; donc si une solution $x \equiv a$ existe, il en existe aussi une seconde $x \equiv p - a \pmod p$.

3. Nous avons vu (III, 14, 15) que pour connaître si une congruence de degré m a m solutions $\pmod p$, il faut prendre le reste de la division de $x^p - x$ par le premier membre de la congruence proposée et s'assurer que les coefficients de ce reste sont $\equiv 0 \pmod p$.

Donc, pour savoir si la congruence $z^2 \equiv q \pmod p$ admet deux solutions ou aucune solution, il faut trouver le reste de la division de $z^p - z$ par $z^2 - q$.

Or

$$z^p - z = z\left[(z^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}}\right] + z\left[q^{\frac{p-1}{2}} - 1\right].$$

Le premier terme

$$z\left[(z^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}}\right]$$

est divisible par $z^2 - q$, donc le reste de la division de $z^2 - p$ par $z^2 - q$ est

$$z\left[q^{\frac{p-1}{2}} - 1\right].$$

Pour que la congruence $z^2 \equiv q \pmod p$ ait deux solutions, il

faut que le coefficient de z soit $\equiv 0 \pmod p$ ou

$$q^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p.$$

Ainsi la congruence $z^2 \equiv 2 \pmod 7$ admet deux solutions, car

$$\frac{7-1}{2} = 3 \quad \text{et} \quad 2^3 \equiv 1 \pmod 7.$$

La congruence $z^2 \equiv 2 \pmod{11}$ n'est pas possible, car $\frac{11-1}{2} = 5$ et $2^5 = 32$ n'est pas $\equiv 0 \pmod{11}$.

4. Inversement, si la congruence $z^2 \equiv q \pmod p$ admet deux solutions

$$z \equiv a \quad \text{et} \quad z \equiv (p-a) \pmod p,$$

on aura

$$q^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

En effet, puisque $z \equiv a$ est une solution de $z^2 \equiv q \pmod p$, on aura $a^2 \equiv q \pmod p$ ou, en élevant les deux membres à une puissance dont l'exposant est $\frac{p-1}{2}$,

$$a^{\frac{2(p-1)}{2}} \equiv q^{\frac{p-1}{2}} \pmod p$$

ou

$$a^{p-1} \equiv q^{\frac{p-1}{2}} \pmod p.$$

Or

$$a^{p-1} \equiv 1 \pmod p;$$

donc

$$q^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

5. Nous avons vu (III, 1) qu'on a toujours

$$q^{p-1} - 1 \equiv 0 \pmod p,$$

ce qu'on peut écrire

$$\left(q^{\frac{p-1}{2}} - 1\right)\left(q^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

On aura donc toujours

$$q^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

Ainsi la valeur absolue de $q^{\frac{p-1}{2}}$ (mod p) est 1.

Nous avons vu que si l'on a

$$q^{\frac{p-1}{2}} \equiv +1 \pmod{p},$$

la congruence $z^2 \equiv p \pmod{p}$ admet deux solutions.

Si l'on a $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, la congruence $z^2 \equiv q \pmod{p}$ n'est pas possible.

On désigne par le symbole $\left(\frac{q}{p}\right)$ la quantité ± 1 ou mieux la quantité $q^{\frac{p-1}{2}}$.

On écrira donc symboliquement :

$$\left(\frac{q}{p}\right) = +1 \quad \text{si} \quad q^{\frac{p-1}{2}} \equiv +1 \pmod{p},$$

$$\left(\frac{q}{p}\right) = -1 \quad \text{si} \quad q^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Ainsi :

$$\left(\frac{2}{7}\right) = +1, \quad \text{car} \quad 2^3 \equiv 1 \pmod{7},$$

$$\left(\frac{2}{11}\right) = -1, \quad \text{car} \quad 2^5 \equiv -1 \pmod{11}.$$

Nous pouvons donc résumer le paragraphe 3 de ce Chapitre en disant que la congruence $z^2 \equiv q \pmod{p}$ est possible et admet deux solutions si

$$\left(\frac{q}{p}\right) = 1.$$

Par contre, cette congruence n'est pas possible si $\left(\frac{q}{p}\right) = -1$.

Dans le premier cas, q sera dit *résidu quadratique* de p; dans le second cas, q est non-résidu quadratique.

Rappelons que p est supposé premier, mais aucune hypothèse n'est faite sur q si ce n'est que $q \not\equiv 0 \pmod{p}$.

6. Théorème. — *On a toujours*

$$\left(\frac{1}{p}\right) = +1$$

et

$$\left(\frac{-1}{p}\right) = +1 \quad \text{si} \quad p \equiv 1 \pmod 4,$$

$$\left(\frac{-1}{p}\right) = -1 \quad \text{si} \quad p \equiv 3 \pmod 4.$$

En effet, on a

$$\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}} \pmod p;$$

donc

$$\left(\frac{1}{p}\right) \equiv 1^{\frac{p-1}{2}} \equiv 1.$$

Si $p \equiv 1 \pmod 4$, posons $p = 4k+1$, alors

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv +1.$$

Si $p \equiv 3 \pmod 4$, posons $p = 4k+3$, alors

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1.$$

Ainsi 1 est toujours un résidu quadratique.

(-1) est résidu quadratique pour tout nombre premier de la forme $4k+1$.

(-1) est un non-résidu quadratique pour tout nombre premier de la forme $4k+3$.

En d'autres termes, la congruence $z^2 \equiv 1 \pmod p$ est toujours possible; la congruence $z^2 \equiv -1 \pmod p$ n'est possible que si le module p est de la forme $4k+1$.

7. Théorème. — *Si* $q = q_1, q_2, q_3, \ldots, q_n$,

$$\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\left(\frac{q_3}{p}\right)\cdots\left(\frac{q_n}{p}\right).$$

En effet, on a

$$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \pmod p.$$

De même que

$$\left(\frac{q_1}{p}\right) \equiv q_1^{\frac{p-1}{2}}, \quad \left(\frac{q_2}{p}\right) \equiv q_2^{\frac{p-1}{2}}, \quad \ldots, \quad \left(\frac{q_n}{p}\right) \equiv q_n^{\frac{p-1}{2}} \pmod p;$$

d'où, en multipliant ces congruences membre à membre,

$$\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_n}{p}\right) \equiv q_1^{\frac{p-1}{2}} q_2^{\frac{p-1}{2}} \cdots q_n^{\frac{p-1}{2}}$$
$$\equiv (q_1 q_2 \cdots q_n)^{\frac{p-1}{2}} \equiv q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}.$$

Ainsi la détermination du symbole $\left(\frac{q}{p}\right)$, quand q n'est pas premier, se ramène à la détermination de ce symbole quand q est premier.

En particulier, remarquons qu'on peut éliminer les facteurs qui entrent dans q avec un exposant pair.

Si, par exemple, $q = a^2 b$,

$$\left(\frac{q}{p}\right) = \left(\frac{b}{p}\right) \pmod{p}.$$

En effet,

$$\left(\frac{q}{p}\right) = \left(\frac{a^2 b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)^2\left(\frac{b}{p}\right) = \left(\frac{b}{p}\right).$$

8. Théorème. — *Si p est de la forme $4k+1$, les nombres q et $-q$ sont tous deux résidus quadratiques ou tous deux non-résidus quadratiques. Si p est de la forme $4k+3$, les deux nombres q et $-q$ sont l'un résidu quadratique et l'autre non-résidu quadratique.*

En effet,

$$\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-q}{p}\right);$$

or (-1) est résidu quadratique si p est de la forme $4k+1$, alors

$$\left(\frac{q}{p}\right) = \left(\frac{-q}{p}\right),$$

c'est-à-dire que les nombres q et $-q$ sont tous deux résidus quadratiques ou tous deux non-résidus quadratiques.

Mais si p est de la forme $4k+3$, alors

$$\left(\frac{-1}{p}\right) = -1 \quad \text{et} \quad \left(\frac{q}{p}\right) = -\left(\frac{-q}{p}\right),$$

c'est-à-dire que si q est résidu quadratique, $(-q)$ est non-résidu

quadratique, et inversement si q est non-résidu quadratique, $(-q)$ est résidu quadratique.

9. Théorème. — *Si* $q \equiv q' \pmod{p}$, *on aura*

$$\left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right).$$

En effet, la congruence $q \equiv q' \pmod{p}$ entraîne celle-ci :

$$q^{\frac{p-1}{2}} \equiv q'^{\frac{p-1}{2}}$$

ou

$$\left(\frac{q}{p}\right) \equiv \left(\frac{q'}{p}\right) \pmod{p}.$$

Or, la valeur absolue de $\left(\frac{q}{p}\right)$ étant 1, la congruence

$$\left(\frac{q}{p}\right) \equiv \left(\frac{q'}{p}\right) \pmod{p}$$

entraîne l'égalité

$$\left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right).$$

10. Théorème. — *Si l'on désigne par* R *un résidu quadratique, et par* N *un non-résidu quadratique, on aura*

$$RR' = R'', \qquad RN = N', \qquad NR = N', \qquad NN' = R,$$

c'est-à-dire que le produit des deux résidus est un résidu, le produit d'un résidu et d'un non-résidu est un non-résidu, le produit de deux non-résidus est un résidu.

En effet, nous avons vu que si $q = q_1 q_2 q_3 \ldots q_n$, on aura

$$\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\left(\frac{q_3}{p}\right)\cdots\left(\frac{q_n}{p}\right).$$

Puisqu'on a par définition

$$\left(\frac{R}{p}\right) = +1 \qquad \text{et} \qquad \left(\frac{N}{p}\right) = -1,$$

on aura

$$\left(\frac{R}{p}\right)\left(\frac{R'}{p}\right)=+1=\left(\frac{R''}{p}\right),\qquad \left(\frac{R}{p}\right)\left(\frac{N}{p}\right)=(+1)(-1)=-1=\left(\frac{N'}{p}\right),$$

$$\left(\frac{N}{p}\right)\left(\frac{R}{p}\right)=(-1)(+1)=-1=\left(\frac{N'}{p}\right)$$

et enfin

$$\left(\frac{N}{p}\right)\left(\frac{N'}{p}\right)=(-1)(-1)=+1=\left(\frac{R}{p}\right).$$

11. Moyennant les théorèmes que nous avons examinés, le caractère de $q\,(\text{mod}\,p)$ ou la détermination du symbole $\left(\frac{q}{p}\right)$ peut toujours se ramener au cas de q inférieur à p et premier.

Pour ce cas (donc quand q et p sont premiers et $q<p$), nous allons démontrer le théorème suivant :

$$\left(\frac{q}{p}\right)=(-1)^k \qquad \text{avec} \qquad k=\mathrm{E}\left(\frac{2q}{p}\right)+\mathrm{E}\left(\frac{4q}{p}\right)+\ldots+\mathrm{E}\frac{(p-1)q}{p},$$

$\mathrm{E}(x)$ *désignant le plus grand nombre entier contenu dans* x.

En effet, nous avons vu (II, 4) que si $r_i\left(i=1, 2, 3, \ldots, \frac{p-1}{2}\right)$ désigne le résidu minimum absolu (mod p) du nombre iq, le signe de r_i est déterminé par le signe de la quantité

$$(-1)^{\frac{2iq}{p}}.$$

On aura donc, en respectant le signe de r_i,

$$r_i\equiv(-1)^{\frac{2iq}{p}}\,iq \qquad (\text{mod}\,p) \qquad \left(i=1, 2, 3, \ldots, \frac{p-1}{2}\right)$$

ou, en explicitant,

$$r_1\equiv(-1)^{\mathrm{E}\left(\frac{2q}{p}\right)}q, \qquad r_2\equiv(-1)^{\mathrm{E}\left(\frac{4q}{p}\right)}2q, \qquad \ldots,$$

$$r_{\frac{p-1}{2}}\equiv(-1)^{\frac{\mathrm{E}(p-1)q}{p}}\,\frac{p-1}{2}\,q \qquad (\text{mod}\,p)$$

ou, en multipliant membre à membre,

$$r_1r_2r_3\ldots r_{\frac{p-1}{2}}\equiv(-1)^k q\;2q\;3q\ldots\frac{p-1}{2}\,q \qquad (\text{mod}\,p).$$

Or, les facteurs $r_1, r_2, r_3, \ldots, r_{\frac{p-1}{2}}$ ne diffèrent que par l'ordre

des facteurs 1, 2, 3, ..., $\frac{p-1}{2}$, car ils sont tous non supérieurs à $\frac{p-1}{2}$ (comme résidus minimums) et sont tous distincts.

Si, en effet, on avait $r_i = r_k$ avec i et k non supérieurs à $\frac{p-1}{2}$, on aurait

$$(-1)^{E\left(\frac{2iq}{p}\right)} iq \equiv (-1)^{E\left(\frac{2kq}{p}\right)} kq \pmod{p},$$

ce qui donnerait

$$iq \equiv \pm kq \pmod{p}$$

et entraînerait la divisibilité de $i \pm k$ par p, ce qui est impossible, i et k étant deux nombres supérieurs à $\frac{p-1}{2}$.

Ainsi

$$r_1 r_2 r_3 \ldots r_{\frac{p-1}{2}} = 1.2.3.4 \ldots \frac{p-1}{2}$$

et

$$r_1 r_2 r_3 \ldots r_{\frac{p-1}{2}} \equiv (-1)^k q\, 2q\, 3q\, 4q \ldots \frac{p-1}{q} \pmod{p}$$

devient, quand on supprime les facteurs communs,

$$1 = (-1)^k q^{\frac{p-1}{2}} \pmod{p}.$$

Si, enfin, on multiplie les deux membres par $(-1)^k$, il vient

$$q^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p},$$

k désignant la quantité

$$(-1)^{E\left(\frac{2q}{p}\right)+E\left(\frac{4q}{p}\right)+\ldots+E\left(\frac{p-1}{p}\right)q}.$$

Ainsi, pour déterminer le caractère de 5 (mod 13), on calculera

$$E\left(\frac{10}{13}\right) = 0, \quad E\left(\frac{20}{13}\right) = 1, \quad E\left(\frac{30}{13}\right) = 2, \quad E\left(\frac{40}{13}\right) = 3,$$

$$E\left(\frac{50}{13}\right) = 3, \quad E\left(\frac{60}{13}\right) = 4,$$

$$k = 0 + 1 + 2 + 3 + 3 + 4 = 13$$

et

$$\left(\frac{5}{13}\right) = (-1)^k = (-1)^{13} = -1.$$

12. La relation précédente est vraie quel que soit q. Elle peut être simplifiée si q est impair. Supposons donc q impair, et remarquons que

$$\left(\frac{q}{p}\right)=\left(\frac{q+p}{p}\right).$$

Si, dans la formule du paragraphe précédent,

$$\left(\frac{q}{p}\right)=(-1)^k, \qquad k=\mathrm{E}\left(\frac{2q}{p}\right)+\mathrm{E}\left(\frac{4q}{p}\right)+\mathrm{E}\left(\frac{6q}{p}\right)+\ldots+\mathrm{E}\,\frac{(p-1)q}{p},$$

on fait

$$q=\frac{1}{2}(p+a),$$

a étant supposé impair (ainsi que p), il vient

$$\left[\frac{\frac{1}{2}(a+p)}{q}\right]=(-1)^{\mathrm{E}\frac{p+a}{p}+\mathrm{E}\frac{2(p+a)}{p}+\ldots+\mathrm{E}\frac{(p-1)(p+a)}{p}}=(-1)^k,$$

et si l'on multiplie les deux membres par $\left(\frac{2}{p}\right)$ et en remarquant que l'exposant de (-1) est

$$\mathrm{E}\left(1+\frac{a}{p}\right)+\mathrm{E}\left(2+\frac{2a}{p}\right)+\ldots+\mathrm{E}\left[p-1+\frac{(p-1)a}{2p}\right]$$

$$=1+2+3+\ldots+\frac{p-1}{2}+\mathrm{E}\frac{a}{p}+\mathrm{E}\frac{2a}{p}+\ldots+\frac{(p-1)a}{2p}$$

$$=\frac{\frac{p+1}{2}\,\frac{p-1}{2}}{2}+\mathrm{E}\left(\frac{a}{p}\right)+\mathrm{E}\left(\frac{2a}{p}\right)+\ldots+\mathrm{E}\frac{(p-1)a}{2p}$$

$$=\frac{p^2-1}{8}+\mathrm{E}\left(\frac{a}{p}\right)+\mathrm{E}\left(\frac{2a}{p}\right)+\ldots+\mathrm{E}\,\frac{(p-1)a}{2p},$$

on trouve

$$\left(\frac{2}{p}\right)\left[\frac{\frac{1}{2}(a+p)}{p}\right]$$
$$=\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)=\left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}+\mathrm{E}\left(\frac{a}{p}\right)+\mathrm{E}\left(\frac{2a}{p}\right)+\ldots+\mathrm{E}\,\frac{(p-1)a}{2p}}.$$

Si l'on fait dans cette relation $a=1$, on trouve

$$\left(\frac{1}{p}\right)=1=\left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}},$$

tous les $E\left(\frac{ia}{p}\right)$ étant nuls et en multipliant cette relation membre à membre avec la précédente, on aura

$$\left(\frac{a}{p}\right) = (-1)^{E\left(\frac{a}{p}\right) + E\left(\frac{2a}{p}\right) + \ldots + E\frac{(p-1)a}{2p}},$$

relation de la même forme que celle du paragraphe précédent, mais dont les termes sont deux fois plus petits.

13. Nous avons trouvé, dans le paragraphe précédent, la relation

$$1 = \left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}}.$$

En multipliant les deux termes par

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p^2-1}{8}},$$

il vient

$$(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{4}},$$

et puisque le carré de tout nombre impair est de la forme $8n+1$, car

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$$

et $k(k+1)$ étant pair, $(2k+1)^2 = 8n+1$; donc $\frac{p^2-1}{4}$ est pair et $(-1)^{\frac{p^2-1}{4}} = +1$; donc on aura

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-}{8}}.$$

Nous avons vu que $\frac{p^2-1}{4}$ est toujours pair si p est impair.

Pour ce qui est du nombre $\frac{p^2-1}{8}$, il peut être pair ou impair suivant que p est de la forme $8k \pm 1$ ou $8k \pm 3$.

Ainsi, si $p = 8k \pm 1$,

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = \text{pair} \quad \text{et} \quad \left(\frac{2}{p}\right) = +1.$$

Mais si $p = 8k \pm 3$,

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 2(4k^2 \pm 3k) + 1 = \text{impair}$$

et

$$\left(\frac{2}{p}\right) = -1.$$

Ainsi, nous avons le théorème :

$$\left(\frac{2}{p}\right) = +1 \quad \text{si} \quad p \equiv \pm 1 \pmod 8,$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{si} \quad p \equiv \pm 3 \pmod 8,$$

ou

$$\left(\frac{2}{8k \pm 1}\right) = +1 \quad \text{et} \quad \left(\frac{2}{8k \pm 3}\right) = -1.$$

Ainsi

$$\left(\frac{2}{17}\right) = +1, \qquad \left(\frac{2}{37}\right) = -1.$$

14. Théorème. — *Si a est impair et inférieur à p, on aura*

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2} - \mathrm{E}\left(\frac{p}{a}\right) - \mathrm{E}\frac{2p}{a} - \ldots - \mathrm{E}\frac{(a-1)p}{2a}}.$$

En effet, nous avons la relation

$$\left(\frac{a}{p}\right) = (-1)^k \quad \text{avec} \quad k = \mathrm{E}\left(\frac{a}{p}\right) + \mathrm{E}\left(\frac{2a}{p}\right) + \ldots + \mathrm{E}\frac{(p-1)a}{2p}.$$

Cherchons la valeur de k. Remarquons, à cet effet, que k est une somme de plusieurs entiers dont le plus petit est

$$\mathrm{E}\left(\frac{a}{p}\right) = 0,$$

et le plus grand

$$\mathrm{E}\frac{(p-1)a}{2p} = \mathrm{E}\left(\frac{a}{2} - \frac{a}{2p}\right) = \mathrm{E}\left(\frac{a-1}{2} + \frac{p-a}{2p}\right) = \frac{a-1}{2}.$$

Ainsi k est une somme de $\frac{p-1}{2}$ nombres croissant de 0 à $\frac{a-1}{2}$.

Pour déterminer cette somme, calculons combien il y a de termes dont la valeur est 0, combien il y a de termes dont la valeur est 1, puis 2, 3, ..., jusqu'à $\frac{a-1}{2}$.

Posons-nous la question d'une façon générale.

Étant donnée la somme

$$k = \mathrm{E}\left(\frac{a}{p}\right) + \mathrm{E}\left(\frac{2a}{p}\right) + \ldots + \mathrm{E}\left(\frac{ya}{p}\right) + \mathrm{E}\,\frac{(y+1)a}{p} + \ldots + \mathrm{E}\,\frac{(p-1)a}{2a},$$

déterminer combien il y a de termes dont la valeur est x, le nombre entier x étant compris entre o et $\frac{a-1}{2}$.

Supposons que le dernier terme inférieur à x soit $\mathrm{E}\left(\frac{ya}{p}\right)$, de sorte qu'on aura

$$\frac{ya}{p} < x < \frac{(y+1)a}{p},$$

ce qui donne

$$y < \frac{px}{a} < y+1,$$

ce qui montre qu'il y a

$$\mathrm{E}\left(\frac{px}{a}\right)$$

nombres dont la valeur est inférieure à x.

On trouvera de la même façon qu'il y a

$$\mathrm{E}\,\frac{p(x+1)}{a}$$

nombres dont la valeur est inférieure à $x+1$.

Il y a donc

$$\mathrm{E}\,\frac{p(x+1)}{a} - \mathrm{E}\,\frac{px}{a}$$

nombres égaux chacun à x.

Ainsi la valeur de k se compose de :

$\mathrm{E}\,\frac{p}{a} - \mathrm{E}\,\frac{0p}{a}$	nombres égaux chacun à	o,
$\mathrm{E}\,\frac{2p}{a} - \mathrm{E}\,\frac{p}{a}$	»	1,
$\mathrm{E}\,\frac{3p}{a} - \mathrm{E}\,\frac{2p}{a}$	»	2,
....		,
$\mathrm{E}\,\frac{\frac{1}{2}(a-1)p}{a} - \mathrm{E}\,\frac{\frac{1}{2}(a-3)p}{a}$	»	$\frac{a-3}{2}$,
$\frac{p-a}{2} - \mathrm{E}\,\frac{\frac{1}{2}(a-1)p}{a}$	»	$\frac{a-1}{2}$.

On trouve ainsi :

$$k = 0\left(\mathrm{E}\frac{p}{a} - \mathrm{E}\frac{0p}{a}\right) + 1\left(\mathrm{E}\frac{2p}{a} - \mathrm{E}\frac{p}{a}\right) + 2\left(\mathrm{E}\frac{3p}{a} - \mathrm{E}\frac{2p}{a}\right) + \ldots$$
$$+ \frac{a-3}{2}\left[\mathrm{E}\frac{\frac{1}{2}(a-1)p}{a} - \mathrm{E}\frac{\frac{1}{2}(a-3)p}{a}\right]$$
$$+ \frac{a-1}{2}\left[\frac{p-1}{2} - \mathrm{E}\frac{\frac{1}{2}(a-1)p}{2}\right],$$

ce qui donne

$$k = \frac{a-1}{2}\,\frac{p-1}{2} - \left[\mathrm{E}\frac{p}{a} + \mathrm{E}\frac{2p}{a} + \mathrm{E}\frac{3p}{a} + \ldots + \mathrm{E}\frac{\frac{1}{2}(a-1)p}{a}\right];$$

ainsi

$$\left(\frac{a}{p}\right) = (-1)^k = (-1)^{\frac{a-1}{2}\frac{p-1}{2} - \left(\mathrm{E}\frac{p}{a} + \mathrm{E}\frac{2p}{a} + \ldots + \mathrm{E}\frac{(a-1)p}{2a}\right)}.$$

15. Théorème. — *Si a et b sont deux nombres premiers impairs et distincts, on aura*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

En effet, on a (IV, 14)

$$\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2} - \left[\mathrm{E}\frac{b}{a} + \mathrm{E}\frac{2b}{a} + \mathrm{E}\frac{3b}{a} + \ldots + \mathrm{E}\frac{(a-1)b}{2a}\right]};$$

d'autre part (IV, 12),

$$\frac{b}{a} = (-1)^{\mathrm{E}\frac{b}{a} + \mathrm{E}\frac{2b}{a} + \ldots + \mathrm{E}\frac{(a-1)b}{2a}},$$

d'où, en multipliant membre à membre,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

C'est en cette formule que consiste la loi de réciprocité des nombres premiers.

On peut encore interpréter la dernière formule d'une autre façon. On a

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

Si donc un des nombres a ou b est de la forme $4k+1$, l'un des facteurs de l'exposant de (-1) sera pair et le second membre est $+1$; donc

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=+1$$

et alors

$$\left(\frac{a}{b}\right)=\left(\frac{b}{a}\right),$$

ce qui revient à dire que le caractère de $\left(\frac{a}{b}\right)$ est le même que celui de $\left(\frac{b}{a}\right)$.

Mais si les deux nombres sont de la forme $4k+3$, l'exposant de (-1) contient deux facteurs impairs et

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=-1 \qquad \text{ou} \qquad \left(\frac{a}{b}=-\right)\left(\frac{b}{a}\right),$$

ce qui revient à dire que si a est résidu (mod b), b est non-résidu (mod a).

16. Ainsi, nous avons établi les résultats suivants :

1° $+1$ est résidu de n'importe quel nombre où $\left(\frac{1}{p}\right)=+1$.

2° -1 est résidu des nombres de la forme $4k+1$ et non-résidu de nombres de la forme $4k+3$.

3° Si p est de la forme $4k+1$, les nombres a et $-a$ sont à la fois tous deux résidus ou tous non-résidus.

4° $$\left(\frac{abc\ldots}{p}=\right)\left(\frac{a}{b}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\cdots$$

5° $$\left(\frac{2}{p}\right)=+1 \quad \text{si} \quad p=8k\pm 1,$$

$$(2)=-1 \quad \text{si} \quad p=8k\pm 3.$$

6° Si l'on désigne par R, R′, R″ des résidus; et par N, N′, N″, ... des non-résidus (mod p), on aura

$$RR'' = R'', \qquad RN = N', \qquad NR = N', \qquad NN' = R.$$

7° Si a et b sont premiers, impairs et distincts, on aura

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\,\frac{b-1}{2}},$$

ou bien on aura toujours

$$\left(\frac{a}{b}\right)=\left(\frac{b}{a}\right),$$

à moins que les nombres a et b ne soient de la forme $4k+3$; alors

$$\left(\frac{a}{b}\right)=-\left(\frac{b}{a}\right).$$

Moyennant ces formules, on peut trouver la valeur du symbole $\left(\frac{a}{b}\right)$ quels que soient a et b, sous la seule condition que b soit premier.

Ainsi :

$$\left(\frac{1813}{601}\right)=\left(\frac{412}{601}\right)=\left(\frac{4.103}{601}\right)=\left(\frac{103}{601}\right)=\left(\frac{601}{103}\right)=\left(\frac{86}{103}\right)$$
$$=\left(\frac{2}{103}\right)\left(\frac{43}{103}\right)=-\left(\frac{103}{43}\right)=-\left(\frac{17}{43}\right)=-\left(\frac{43}{17}\right)=-\left(\frac{9}{17}\right)=-1.$$

17. Avant de continuer l'extension de cette théorie pour le cas d'un module composé ou d'un module 2^n, il est bon d'envisager toute la question sous un autre point de vue.

Nous avons défini le symbole $\left(\frac{a}{b}\right)$ par la congruence

$$\left(\frac{a}{b}\right)\equiv a^{\frac{b-1}{2}} \pmod p$$

et avons démontré que si $\left(\frac{a}{b}\right)=1$, la congruence $x^2\equiv a \pmod b$ admet deux solutions. On peut aussi arriver à la définition du symbole $\left(\frac{a}{b}\right)$ d'une autre manière.

Tout nombre est congru à l'un des nombres $0.1.2.3\ldots(p-1)$ $(\text{mod } p)$; donc, quel que soit x, on aura

$$x\equiv 0.1.2.3\ldots(p-2) \text{ ou } (p-1) \pmod p.$$

Si l'on élève tous ces nombres au carré, on aura non pas p valeurs différentes de x^2, mais

$$\frac{p+1}{2} \text{ valeurs différentes,}$$

et si, provisoirement, on exclut la valeur $x = 0$ [donc aussi la valeur $x^2 \equiv 0 \pmod p$], on aura $p - 1$ valeurs différentes de x, mais

$$\frac{p-1}{2} \text{ valeurs différentes de } x^2,$$

car il existe toujours deux valeurs x et $(p - x)$ dont les carrés sont les mêmes $\pmod p$, puisque $x^2 \equiv (p - x)^2 \pmod p$.

Ainsi $p = 7$ donne

$$x \equiv 1.2.3.4.5.6 \quad \pmod 7,$$
$$x^2 \equiv 1.4.2.2.4.1 \quad \pmod 7.$$

Ainsi, quel que soit x, non divisible par 7, on aura toujours

$$x^2 \equiv 1 \text{ ou } 4 \text{ ou } 2 \quad \pmod 7.$$

Donc, pour le module 7, les nombres 1, 2 et 4 sont des résidus quadratiques; les autres nombres de la série 1.2.3.4.5.6 autres que 1.2.4, c'est-à-dire les nombres 3.5.6, sont les non-résidus et la congruence $x^2 \equiv 3.5$ ou $6 \pmod 7$ est impossible. Ainsi un nombre de la forme $7k + 3$ ou $7k + 5$ ou $7k + 6$ ne peut jamais devenir un carré.

Quelques-unes de ces notions sont connues dans l'arithmétique élémentaire. Ainsi aucun carré ne peut finir par les chiffres 2.3.7 ou 8, car un nombre qui finit par ces chiffres est $\equiv 2$ ou $3 \pmod 5$ et 2 et 3 sont non-résidus $\pmod 5$.

Il est évident que, pour un module donné, il y a autant de résidus que de non-résidus.

18. Toujours en excluant la valeur 0 pour le nombre considéré et la valeur 2^n pour le module, prenons pour module une puissance d'un nombre premier impair et voyons quels sont les résidus $\pmod{p^n}$.

Il est facile de démontrer que tout résidu $\pmod p$ est aussi résidu $\pmod{p^n}$ et, inversement, tout résidu $\pmod{p^n}$ est également résidu $\pmod p$.

En effet, supposons que

$$\left(\frac{a}{p}\right) = +1;$$

je dis qu'on aura aussi $\left(\frac{N}{p^2}\right) = +1$ et, d'une manière générale,

$$\left(\frac{N}{p^n}\right) = +1 \quad \text{si} \quad N \equiv a \pmod{p}.$$

Si $\left(\frac{a}{p}\right) = 1$, on peut trouver un nombre x tel que $x^2 \equiv a \pmod{p}$.

Nous allons prouver qu'on peut aussi résoudre la congruence

$$y^2 \equiv a + pk \pmod{p^2}.$$

Si l'on pose $y = pz + x \pmod{p^2}$, x étant déterminé par la congruence $x^2 \equiv a \pmod{p}$, il vient

$$y^2 \equiv p^2z^2 + 2pzx + x^2 \equiv 2pzx + a \pmod{p^2}.$$

La congruence donnée $y^2 \equiv a + pk \pmod{p^2}$ devient

$$2pzx + a \equiv a + pk \pmod{p^2}$$

ou

$$2zx \equiv k \pmod{p},$$

congruence qui est toujours possible puisque p est premier.

De proche en proche on peut s'assurer que, si $\left(\frac{a}{p}\right) = 1$, la congruence

$$x^2 = a + bp + cp^2 + \ldots + kp^{n-1} \pmod{p^n}$$

est toujours possible et n'admet que deux solutions $(\bmod p^n)$.

19. Examinons maintenant la valeur de o pour un module p^n, p étant supposé premier impair.

Il est évident que o est résidu $(\bmod p)$.

Mais $a \equiv 0 \pmod{p}$ peut donner $a \equiv kp \pmod{p^2}$ et il est évident que a n'est résidu que si $k = 0$, c'est-à-dire de tous les nombres $\equiv 0 \pmod{p}$ tels que $\equiv 0, p, 2p, \ldots, (p-1)p \pmod{p^2}$, seul le premier est résidu $(\bmod p^2)$.

Si l'on désigne par $r_1 r_2 r_3 \ldots r_i \left(i = \frac{p-1}{2}\right)$ tous les résidus différents de o $(\bmod p)$, on aura :

Résidu $(\bmod p)$:

$$x \equiv 0 r_1 r_2 r_3 \ldots r_i;$$

Résidus $(\bmod p^2)$:

$$x \equiv r_1 r_3 . \; . r_i \pmod{p} \quad \text{et} \quad x \equiv 0 \pmod{p^2};$$

Résidus (mod p^3) :

$$x \equiv r_1 r_2 \dots r_i \pmod p \quad \text{et} \quad x \equiv 0 \quad \text{ou} \quad p^2 r_i \pmod{p^3}$$
$$\left(i = 1, 2, 3, \dots, \frac{p-1}{2}\right);$$

Etc.

Ainsi $a \equiv 0 \pmod{p^n}$ n'est résidu que si

$$a \equiv p^{2k} r_i \pmod{p^n} \quad \text{et} \quad \left(\frac{r_i}{p}\right) = +1,$$

r_i pouvant du reste être o.

Exemple. — $p = 5$ donne les résidus suivants :

Module 5 :

$$r \equiv 0, 1 \text{ ou } 4;$$

Module 25 :

$$r \equiv 1 \text{ ou } 4 \pmod 5 \quad \text{ou} \quad \equiv 0 \pmod{25},$$

soit en tout 11 résidus (mod 25);

Module 125 :

$$r \equiv 1 \text{ ou } 4 \pmod 5 \quad \text{ou} \quad 0.25.100 \pmod{125},$$

soit en tout 53 résidus (mod 125);

Module 625 :

$$r \equiv 1 \text{ ou } 4 \pmod 5 \quad \text{ou} \quad 0.25(5k \pm 1),$$

soit en tout 261 résidus (mod 625);

Etc.

20. Il nous reste à examiner le cas de $p = 2^n$.

D'abord pour $n = 1$ le module est 2 et tout nombre est résidu. Cela résulte aussi du (III, 13) puisque dans ce cas la congruence $x^2 \equiv q \pmod p$ peut être remplacée par une congruence du premier degré, toujours possible.

Si $n = 2$, $p = 4$ et le seul résidu impair est 1, le seul résidu pair est o (mod 4).

Si $n = 3$, $p = 8$. Puisque tout carré impair est de la forme $8k + 1$, le seul résidu impair est $+1$, les résidus pairs sont $0.4 \pmod 8$.

En reprenant ensuite ce qui est dit au paragraphe précédent, on

trouve que, quel que soit le module 2^n, avec n non inférieur à 3, les résidus impairs sont $8k+1$ et les résidus pairs $2^{2a}(8k+1)$ ou 0 (mod 2^{ν}).

21. Voyons maintenant quels sont les résidus pour un nombre composé $p = abc\ldots$. Il est évident que si N est un résidu de p, il sera aussi résidu de tout diviseur de p, donc de $a.b.c\ldots$. Inversement, tout résidu de $a.b.c\ldots$ sera aussi résidu de leur produit p. Cette dernière conclusion se démontre facilement de la façon suivante : Si N est résidu de $a.b.c\ldots$, on peut résoudre les congruences :

$$x^2 \equiv \mathrm{N} \pmod{a},$$
$$x^2 \equiv \mathrm{N} \pmod{b},$$
$$x^2 \equiv \mathrm{N} \pmod{c},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

Si

$$x \equiv r_1 \pmod{a}, \qquad x \equiv r_2 \pmod{b}, \qquad x \equiv r_3 \pmod{c}$$

sont des solutions de ces congruences, on peut trouver un nombre $x \equiv \mathrm{R} \pmod{p}$ qui remplace les solutions trouvées (II, 13, 16). Mais si N n'est pas résidu d'un ou plusieurs facteurs, il n'est pas résidu de leur produit.

Jacobi représente par le symbole de Legendre $\left(\frac{q}{p}\right)$ le caractère de q (mod p), quel que soit p, donc même si p n'est pas premier, tandis que Legendre n'a introduit ce symbole rien que pour le cas de p premier.

Voici la définition de Jacobi : Si $p = ab$, $\left(\frac{q}{p}\right) = \left(\frac{q}{a}\right)\left(\frac{q}{b}\right)$.

Moyennant certains théorèmes auxiliaires, faciles du reste à établir, Jacobi trouve pour son symbole $\left(\frac{q}{p}\right)$ les mêmes formules que nous avons trouvées pour le symbole $\left(\frac{q}{p}\right)$ de Legendre.

Ainsi, pour fixer les idées, considérons le symbole $\left(\frac{2}{p}\right)$.

Nous avons vu que si $p = 8k+1$, $\left(\frac{2}{p}\right) = +1$, et $\left(\frac{2}{p}\right) = -1$, si $p = 8k \pm 3$.

Supposons maintenant que p n'est pas premier et soit $p = ab$. Les cas suivants peuvent se présenter (mod 8) :

1° $p \equiv 1$:

a	$\equiv 1$	3	5	7
b	$\equiv 1$	3	5	7
$\left(\frac{2}{a}\right)$	$\equiv +1$	-1	-1	$+1$
$\left(\frac{2}{b}\right)$	$\equiv +1$	-1	-1	$+1$

2° $p \equiv 7$:

a	$\equiv 1$	3	5	7
b	$\equiv 7$	5	3	1
$\left(\frac{2}{a}\right)$	$\equiv +1$	-1	-1	$+1$
$\left(\frac{2}{b}\right)$	$\equiv +1$	-1	-1	$+1$

Dans tous les cas,

$$\left(\frac{2}{p}\right) = \left(\frac{2}{a}\right)\left(\frac{2}{b}\right) = +1$$

tout comme si p était premier.

3° $p \equiv 3$:

a	$\equiv 1$	3	5	7
b	$\equiv 3$	1	7	5
$\left(\frac{2}{a}\right)$	$\equiv 1$	-1	-1	$+1$
$\left(\frac{2}{b}\right)$	$\equiv -1$	$+1$	$+1$	-1

4° $p \equiv 5$:

a	$\equiv 1$	3	5	7
b	$\equiv 5$	7	1	3
$\left(\frac{2}{a}\right)$	$\equiv +1$	-1	-1	$+1$
$\left(\frac{2}{b}\right)$	$\equiv -1$	$+1$	$+1$	-1

et

$$\left(\frac{2}{p}\right) = \left(\frac{2}{a}\right)\left(\frac{2}{b}\right) = -1$$

comme si p était premier.

Ainsi le symbole $\left(\frac{2}{p}\right)$ peut se calculer par la règle connue (IV, 13) quel que soit p.

Remarquons cependant que si l'on ne connaît pas la nature du nombre p, on n'est pas avancé par le calcul du symbole $\left(\frac{a}{p}\right)$.

En effet, si l'on trouve $\left(\frac{a}{p}\right) = +1$, a n'est résidu de p que si p est premier ou composé de facteurs pour chacun desquels a est résidu. Mais si p contient deux facteurs (ou en général un nombre pair de facteurs) et que a n'est pas résidu de ces facteurs, on trouvera aussi $\left(\frac{a}{p}\right) = +1$ sans que a soit résidu de p, donc sans que la congruence $x^2 \equiv a \pmod{p}$ soit possible.

Si, cependant, on trouve $\left(\frac{a}{p}\right) = -1$, a n'est jamais un résidu de p quel que soit p (premier ou composé).

22. *Application.* — Trouver les derniers chiffres d'un carré.

Le dernier chiffre d'un carré est x tel que $\left(\frac{x}{10}\right) = +1$, condition qui exige

$$\left(\frac{x}{2}\right) = +1 \quad \text{et} \quad \left(\frac{x}{5}\right) = +1.$$

Or $\left(\frac{x}{2}\right) = +1$ est toujours vérifié et $\left(\frac{x}{5}\right) = +1$ est vérifié pour $x \equiv 0.1.4 \pmod{5}$.

On aura donc

$$x \equiv 0.1.4 \pmod{5} \quad \text{ou} \quad x \equiv 0.1.4.5.6.9 \pmod{10}.$$

Le dernier chiffre d'un carré est donc 0.1.4.5.6 ou 9.

Les deux derniers chiffres d'un carré sont tels qu'ils forment un nombre x et

$$\left(\frac{x}{100}\right) = +1,$$

conditions équivalentes aux deux suivantes :

$$\left(\frac{x}{4}\right) = +1 \quad \text{et} \quad \left(\frac{x}{25}\right) = +1.$$

Or $\left(\frac{x}{4}\right) = +1$ est vérifié pour $x \equiv 0.1 \pmod{4}$ et $\left(\frac{x}{25}\right) = +1$ est

vérifié pour $x \equiv 1.4 \pmod 5$ ou $x \equiv 0 \pmod{25}$ soit pour 11 valeurs (mod 25).

On trouvera donc

$$2 \times 11 = 22 \text{ valeurs de } x \pmod{100}.$$

On trouve :

$$X \equiv 00.01.04.09.16.21.24.25.29.36.41.44.49.56.61.64.$$
$$69.76.81.84.89.96 \pmod{100}.$$

On trouvera les trois derniers chiffres par la condition

$$\left(\frac{x}{1000}\right) = +1 \quad \text{ou} \quad \left(\frac{x}{8}\right) = +1 \quad \text{et} \quad \left(\frac{x}{125}\right) = +1.$$

Les solutions de $\left(\frac{x}{8}\right) = +1$ sont

$$x \equiv 0.1.4 \pmod 8).$$

Les solutions de $\left(\frac{x}{125}\right) = +1$ sont

$$x \equiv 1.4 \pmod 5 \quad \text{ou} \quad 0.25.100 \pmod{125},$$

soit pour 53 valeurs de x (mod 125), d'où il résulte

$$3 \times 53 = 159 \text{ solutions} \quad (\text{mod } 8 \times 125 = 1000).$$

Les quatre derniers chiffres s'obtiennent par la condition

$$\left(\frac{x}{10000}\right) = +1$$

ou

$$\left(\frac{x}{16}\right) = +1 \quad \text{et} \quad \left(\frac{x}{625}\right) = +1.$$

Or $\left(\frac{x}{16}\right) = +1$ est vérifié pour

$$x \equiv 0.1.4.9 \pmod{16}$$

et $\left(\frac{x}{625}\right) = +1$ est vérifié pour

$$x \equiv 1.4 \pmod 5 \text{ ou } 0 \text{ ou } 25\,(5k \pm 1) \pmod{625},$$

soit pour 261 valeurs de x (mod 625).

On aura donc en tout $4 \times 261 = 1044$ solutions (mod 10000).

On peut grouper ces 1044 solutions de la façon suivante :

Si les deux derniers chiffres sont :	Les deux avant-derniers seront tels que :			
00	$\left(\frac{x}{100}\right) = +1$,	d'où	22	solutions
01.09.41.49.81.89	$2k$,	»	300	»
21.29.61.69	$4k+1$,	»	200	»
04.36.84	$4k+0.3$,	»	150	»
24.56	$4k+2.3$,	»	100	»
16.64.96	$4k+0.1$,	»	150	»
44.76	$4k+1.2$,	»	100	»
25	$10k+0.2$	»	22	»
	ou $50k+6$	»		
	soit en tout :		1044	solutions

23. Pour terminer, nous donnons (Table IV) une Table de résidus pour tous les modules p premiers et inférieurs à 200. Ce sont les solutions de la congruence symbolique $\left(\frac{x}{p}\right) = +1$. Les nombres qui manquent dans cette Table sont solutions de la congruence

$$\left(\frac{x}{p}\right) = -1.$$

Pour former cette Table, on peut cribler tous les nombres inférieurs à p. Ainsi, avec $p = 13$, on aura :

$$\left(\frac{1}{p}\right) = +1, \quad \left(\frac{3}{p}\right) = \left(\frac{1}{3}\right) = +1, \quad \left(\frac{4}{p}\right) = +1, \quad \left(\frac{9}{p}\right) = +1,$$

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = +1,$$

$$\left(\frac{12}{p}\right) = \left(\frac{4.3}{p}\right) = \left(\frac{3}{p}\right) = +1,$$

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{5}{p}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1,$$

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)(+1) = -1,$$

$$\left(\frac{7}{p}\right) = \left(\frac{6}{7}\right) = -\left(\frac{+1}{7}\right) = -1, \quad \left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^3 = -1,$$

$$\left(\frac{11}{p}\right) = \left(\frac{2}{11}\right) = -1.$$

Ainsi les seuls résidus sont 1.3.4.9.10 et 12.

Il est plus simple d'élever au carré les nombres

$$x \equiv 1.2.3.4.5.6 \pmod{13},$$

on trouve

$$x^2 \equiv 1.4.9.3.12.10 \pmod{13},$$

d'où la même série de résidus.

24. Ayant reconnu que

$$\left(\frac{a}{p}\right) = +1,$$

on est certain que la congruence $x^2 \equiv a \pmod{p}$ est possible et admet deux solutions, si p est premier.

Nous allons nous occuper maintenant de la résolution effective de cette congruence.

Remarquons d'abord que si le module p n'est pas premier, on transformera la congruence donnée en d'autres dont les modules sont premiers ou puissances de nombres premiers.

Soit donc p premier et $x^2 \equiv a \pmod{p}$, la congruence donnée.

En excluant le cas où a est un carré parfait $a = b^2$, ce qui donne immédiatement $x^2 \equiv \pm b \pmod{p}$, on ne connaît la solution directe que dans les trois cas que voici :

1° $a \equiv -1$. — Il faut alors que p soit de la forme $4k+1$, car autrement $\left(\frac{a}{p}\right)$ ne serait pas égal à $+1$.

D'après le théorème de Wilson, on a (III, 9)

$$1.2.3\ldots(4k)+1 \equiv 0 \pmod{p}$$

ou

$$[1.2.3\ldots(2k)]^2 \equiv -1 \pmod{p}.$$

En comparant ce résultat avec la congruence donnée

$$x^2 \equiv -1 \pmod{p},$$

on voit qu'on peut prendre

$$x \equiv \pm[1.2.3\ldots(2k)] \pmod{p}.$$

Cette solution directe est bien plus compliquée que la solution par tâtonnement que nous verrons plus loin (IV, 25).

2° Si p est de la forme $4k+3$, on peut encore trouver la solution de la congruence $x^2 \equiv a \pmod{p}$.

En effet, cette congruence étant supposée possible, on a

$$\left(\frac{a}{p}\right) = +1 \quad \text{ou} \quad a^{\frac{p-1}{2}} \equiv a^{2k+1} \equiv 1 \pmod{p}$$

ou

$$a^{2k+2} \equiv a \pmod{p}, \quad \text{d'où} \quad x \equiv \pm a^{k+1} \pmod{p}.$$

Par exemple, si $p = 191$, $\left(\frac{2}{p}\right) = +1$, pour résoudre la congruence $x^2 \equiv 2 \pmod{191}$, on prendra

$$x \equiv \pm 2^{48} \pmod{191}.$$

Or

$$2^{12} \equiv 4096 \equiv 85 \pmod{191},$$
$$2^{24} \equiv 85^2 \equiv 7225 \equiv 158 \equiv -33,$$
$$2^{48} \equiv (-33)^2 \equiv 1089 \equiv 134;$$

ainsi

$$x \equiv \pm 134 \quad \text{ou} \quad x \equiv \pm 57 \pmod{191}.$$

3° On peut encore trouver une solution directe dans le cas de

$$p = 8k+5.$$

Nous verrons (IV, 39) qu'alors p peut être mis sous la forme $p = m^2 + n^2$.

Soit donc $x^2 \equiv a \pmod{p = 8k+5}$, la congruence donnée supposée possible, donc

$$\left(\frac{a}{p}\right) = +1 \quad \text{ou} \quad a^{4k+2} \equiv +1,$$

ce qui donne

$$a^{2k+1} \equiv \pm 1.$$

Cela étant, considérons les deux cas qui peuvent se présenter :

1° Si l'on obtient $a^{2k+1} \equiv +1$, on aura

$$a^{2k+2} \equiv a, \quad \text{d'où} \quad x \equiv \pm a^{k+1};$$

2° Si l'on obtient $a^{2k+1} \equiv -1$, posons

$$M = a^{k+1},$$

ce qui donne

$$M^2 = a^{2k+2} \equiv -a.$$

Supposons encore effectuée la décomposition du module p en somme de deux carrés $p = m^2 + n^2$.

Si maintenant on détermine deux nombres u et v soumis à la condition $mu - nv = \mathrm{M}$, on aura la solution sous la forme

$$x \equiv \pm (mv + nu) \quad (\mathrm{mod}\ p).$$

En effet, on aura

$$\mathrm{X}^2 + \mathrm{M}^2 = (mv + nu)^2 + (mu - nv)^2 = (u^2 + v^2)(m^2 + n^2) = p(u^2 + v^2);$$

or

$$\mathrm{M}^2 \equiv - a \quad (\mathrm{mod}\ p);$$

donc on aura

$$x^2 - a \equiv 0 \quad (\mathrm{mod}\ p).$$

Excepté les trois cas envisagés, on ne peut résoudre la congruence $x^2 \equiv (\mathrm{mod}\ p)$ que par tâtonnement.

25. Soient donc p un module premier, et a résidu de p,

$$x^2 \equiv a \quad (\mathrm{mod}\ p),$$

la congruence donnée.

Transformons la congruence donnée $x^2 \equiv a\,(\mathrm{mod}\ p)$ en équation

$$x^2 = py + a.$$

Cette dernière sera à son tour remplacée par des congruences de modules différents pour trouver les formes linéaires de x pour différents modules.

Remarquons d'abord que x aura deux solutions $(\mathrm{mod}\ p)$ dont une est inférieure à $\frac{p}{2}$. Il existe donc une valeur de y inférieure à $\frac{p}{4}$ qui rend l'expression $py + a$ carré parfait. C'est cette valeur de y que nous cherchons.

Soit m un module tel que 2 ou 2^n, 3 ou 3^n, 5 ou 5^n, 7, 11, 13, 17, 19, ... et donnons à y toutes les valeurs possibles $0.1.2.3\ldots(m-1)$ pour ce module

$$y \equiv 0.1.2.3\ldots(m-1) \quad (\mathrm{mod}\ m).$$

Calculons la valeur correspondante $(\mathrm{mod}\ m)$ de $x^2 \equiv py + a$, il

vient

$$x^2 \equiv a_1 a_2 a_3 \ldots a_m \pmod{m}.$$

Or certaines de ces valeurs a_i sont résidus $(\bmod m)$; certaines autres sont non-résidus. Si, pour $y = k \pmod{m}$, on obtient pour x^2 un non-résidu, la valeur $y = k \pmod{m}$ ne peut pas rendre $py + a$ carré parfait et est, par conséquent, inadmissible.

Sont seules admissibles les valeurs de y qui donnent pour x^2 un résidu.

On trouvera ainsi plusieurs formes linéaires de y qui détermineront y et ensuite x (II, 20).

Exemple. — Soit la congruence

$$x^2 \equiv 2 \pmod{10321}.$$

Elle est possible car

$$\left(\frac{2}{10321}\right) = +1.$$

On la transforme en équation $x^2 = 10321\,y + 2$ qui a une solution $0 < y < \frac{p}{4}$ ou $0 < y < 2580$.

Posons

$$\begin{aligned} y &\equiv 0.1.2.3 \pmod{4}, \\ x^2 &\equiv 2.3.0.1, \\ &\quad n\ n\ r\ r. \end{aligned}$$

(Nous désignons par r un résidu et par n un non-résidu). Puisque $y \equiv 0.1 \pmod{4}$ conduisent à un non-résidu, ces valeurs sont à éliminer et l'on aura

$$y \equiv 2.3 \pmod{4}.$$

On peut même serrer de plus près l'élimination et développer ces deux solutions (mod 4) en huit solutions (mod 16) :

$$\begin{aligned} y &\equiv 2.3.6.7.10.11.14.15 \pmod{16}, \\ x^2 &\equiv 4.5.8.9.12.13.\ 0.\ 1, \\ &\quad r\ n\ n\ r\ n\ \ n\ \ r\ \ r, \end{aligned}$$

dont quatre seules sont admissibles.

On trouve ainsi

$$y \equiv 2.7.14.15 \pmod{16}.$$

Si, de même, on a recours à d'autres modules, on trouvera une série de formes linéaires telles que les suivantes :

Module.	Formes linéaires de y.
16	2.7.14.15
25	2.4 (mod 5) ou 13 (mod 25)
9	2 (mod 3) ou 1 (mod 9)
7	0.2.3.4
11	1.3.4.6.7.8
13	1.2.3.5.6.11.12
17	0.1.3.7.8.12.14.15.16
...	...

Par le procédé que nous avons indiqué (II, 20), on trouve la solution $y = 1799$ donnant $x = 4309$.

Nous verrons dans la suite comment on trouve une solution sans tâtonnement quand on possède une Table d'indices pour le module considéré (V, 13).

26. Supposons maintenant que le module soit une puissance d'un nombre premier impair $p = k^n$.

Si a est différent de o et $\left(\frac{a}{k}\right) = +1$, la congruence

$$x^2 \equiv a \pmod{k^n}$$

est possible. La façon la plus simple pour la résoudre est la suivante :

On commencera par résoudre la congruence $x^2 \equiv a \pmod{k}$. Si $x \equiv b \pmod{k}$ en est la solution, on posera

$$x \equiv ky + b \pmod{k^2} \quad \text{et} \quad (ky + b)^2 \equiv a \pmod{k^2}.$$

On aura une congruence du premier degré pour déterminer y. Connaissant y [donc $x \equiv ky + b \equiv c \pmod{k^2}$], on posera

$$x \equiv k^2 z + c \pmod{k^3} \quad \text{et} \quad (k^2 z + c)^2 \equiv a \pmod{k^3}.$$

On aura donc une congruence du premier degré pour déterminer z. On continuera ainsi jusqu'à ce qu'on arrive au module k^n.

Si $a = 0$, la congruence n'est possible que si $a \equiv 0 \pmod{k^2}$. En posant alors $x = ky$, on aura une congruence de la forme précédente dont le module sera k^{n-2}.

Exemple :

$$x^2 \equiv 4351306 \quad (\text{mod } 9765625 = 5^{10}).$$

Elle donne (mod 5) :

$$y^2 \equiv 1, \quad \text{d'où} \quad y \equiv \pm 1.$$

Il suffit, du reste, de prendre un seul signe, soit $y \equiv +1$.

(Mod 25) :

$$(5z+1)^2 \equiv 6, \quad \text{d'où} \quad 10z+1 \equiv 6, \quad 10z \equiv 5,$$

d'où

$$z \equiv 3 \quad (\text{mod } 5) \quad \text{et} \quad 5z+1 \equiv 16 \text{ ou } 9.$$

(Mod 125) :

$$(25u+9)^2 = 56 \quad \text{ou} \quad 450u \equiv 100 \quad (\text{mod } 125) \quad \text{ou} \quad 9u \equiv 2 \quad (\text{mod } 5),$$

d'où

$$u \equiv 3 \quad (\text{mod } 5) \quad \text{et} \quad 25u+9 \equiv 84 \text{ ou } 41 \quad (\text{mod } 125).$$

(Mod 5^4) :

$$(125t+41)^2 \equiv 56 \quad (\text{mod } 625) \quad \text{ou} \quad 250.41t+1681 \equiv 56 \quad (\text{mod } 625)$$

$$\text{ou} \quad 250.41t \equiv 250 \quad (\text{mod } 625),$$

ce qui donne

$$41t \equiv 1 \quad (\text{mod } 5), \quad \text{d'où} \quad t \equiv 1 \quad (\text{mod } 5)$$

et $125t+41$ devient 166 (mod 625).

En continuant ainsi, on trouve la solution

$$x \equiv \pm 4218291 \quad (\text{mod } 5^{10}).$$

27. Voyons maintenant comment se représente la solution de la congruence

$$x^2 \equiv a \quad (\text{mod } p) \quad \text{avec} \quad p = 2^n.$$

D'abord, pour $n = 1$, la solution est immédiate, étant donné que tout nombre est résidu ; donc

$$x \equiv 1 \quad (\text{mod } 2) \quad \text{si} \quad a \equiv 1,$$
$$x \equiv 0 \quad (\text{mod } 2) \quad \text{si} \quad a \equiv 0.$$

Si $n = 2$, le seul résidu pair est 0 et le seul résidu impair est $+1$.

Si $a \equiv 1 \pmod 4$, on aura

$$x = \text{impair} \quad \text{ou} \quad \equiv 1 \pmod 2;$$

si $a \equiv 0$, on aura

$$x = \text{pair},$$

et si $a \equiv 2$ ou 3, la congruence est impossible.

Dans tous les autres cas, on divisera a, s'il est pair, par une puissance paire de 2.

Si, après avoir divisé a par une puissance paire de 2, on obtient un nombre de la forme $8k+1$, la congruence est possible. Soit $a = 2^{2k}(8n+1)$.

Pour résoudre $x^2 \equiv a \pmod{2^n}$, on posera

$$x = 2^k y$$

et l'on aura

$$y^2 \equiv 8n+1 \pmod{2^{n-2k}}.$$

Nous nous occupons donc du cas, quand n est supérieur à 3 et a impair $\equiv 1 \pmod 8$,

$$x^2 \equiv a \pmod{2^n}.$$

Il existe alors deux valeurs $\pmod{2^{n-1}}$, donc quatre valeurs $\pmod{2^n}$ qui peuvent satisfaire à la congruence donnée.

En effet, on a

$$(2^k \pm x)^2 \equiv x^2 \pmod{2^{k+1}}.$$

Il en résulte qu'en choisissant convenablement la valeur de y, on aura

$$x \equiv (2^{n-1} \pm y) \quad \text{et} \quad x^2 \equiv a \pmod{2^n}.$$

Exemple :

$$x^2 \equiv 113 \pmod{128}$$

donne

$$x \equiv \pm 25 \pmod{64} \quad \text{ou} \quad 4 \text{ solutions} \pmod{128}.$$

On trouve

$$x \equiv 25.39.89.103 \pmod{128}.$$

28. *Applications.* — 1° Trouver les n derniers chiffres d'un nombre, connaissant les n derniers chiffres de son carré.

Le problème revient à résoudre la congruence $x^2 \equiv N \pmod{10^n}$

qui se décompose en deux congruences :

$$x^2 \equiv N \pmod{2^n} \quad \text{et} \quad x^2 \equiv N \pmod{5^n}.$$

La première donne deux solutions $(\text{mod } 2^{n-1})$ ou quatre solutions du $(\text{mod } 2^n)$; la deuxième donne toujours deux solutions $(\text{mod } 5^n)$. On aura donc en tout huit solutions $(\text{mod } 10^n)$.

2° Trouver un nombre qui finisse avec les mêmes n chiffres que son carré (on fait abstraction du nombre $10^n + 0$ et $10^n + 1$).

Soit x le chiffre d'unités. On aura

$$(10.k + x)^2 \equiv x \pmod{10} \quad \text{ou} \quad x^2 \equiv x,$$

d'où

$$x \equiv 0 \text{ ou } 1 \pmod{2 \text{ et } 5} \quad \text{ou} \quad x \equiv 0.1.5.6 \pmod{10}.$$

Les cas de $x \equiv 0$ et $x \equiv 1$ (conduisant aux nombres $10^n + 0$ et $10^n + 1$) étant exclus, développons les deux autres cas.

Soit y le chiffre de dizaines. On aura

$$(10y + 5)^2 = 10y + 5 \pmod{100}, \quad \text{d'où} \quad y \equiv 2 \pmod{10},$$
$$(10y + 6)^2 = 10y + 6 \quad » \quad » \quad y \equiv 7 \quad »$$

Les deux premiers chiffres sont ainsi 25 ou 76.

Soit z le chiffre des centaines. On aura

$$(100z + 25)^2 = 100z + 25 \pmod{1000}, \quad \text{d'où} \quad z \equiv 6 \pmod{10},$$
$$(100z + 76)^2 = 100z + 76 \quad » \quad » \quad z \equiv 3 \quad »$$

En continuant, on trouve les dix chiffres suivants :

$$8212890625 \quad \text{et} \quad 1787109376 \pmod{10^{10}}$$

(*voir* Dickson, *History of the Theory of numbers*, vol. I, p. 458).

29. Occupons-nous maintenant de la question inverse, à savoir :

Un nombre a étant donné, trouver les nombres pour lesquels

$$\left(\frac{a}{x}\right) = +1 \quad \text{ou} \quad \left(\frac{a}{x}\right) = -1,$$

c'est-à-dire trouver tous les nombres pour lesquels il est résidu ou non-résidu.

Nous excluons le cas de $a \equiv 0$, ainsi que le cas de a carré parfait. Ces deux cas ne présentent aucune difficulté, ni d'ailleurs aucun intérêt, car o ainsi que k^2 est résidu de n'importe quel nombre.

Remarquons que, dans ce qui précède, nous avons la solution de ce problème dans certains cas. Ainsi nous savons (IV, 6) que -1 est résidu de tous les nombres de la forme $4k+1$ et non-résidu des nombres de la forme $4k+3$.

Ainsi la solution de $\left(\frac{-1}{x}\right) = +1$ est

$$x \equiv 1 \pmod 4,$$

la solution de $\left(\frac{-1}{x}\right) = -1$ est

$$x \equiv 4k+3,$$

la solution étant supposée être un nombre premier.

De même (IV, 13) on aura la solution de $\left(\frac{2}{x}\right) = +1$ avec $x \equiv 8k+1$, et $\left(\frac{2}{x}\right) \equiv -1$ donnera

$$x \equiv \pm 3 \pmod 8.$$

Nous allons démontrer quelques théorèmes qui nous faciliteront la solution de ce problème pour d'autres cas.

30. Théorème. — *Si a est positif et de la forme $4k+1$* (premier ou non), *on aura*

$$\left(\frac{a}{2na+x}\right) = \left(\frac{a}{2na-x}\right) = \frac{a}{x},$$

à la condition que x ainsi que $2na \pm x$ soient premiers.

En effet, si a est premier, on a

$$\left(\frac{a}{2na \pm x}\right) = \left(\frac{2na \pm x}{a}\right) = \left(\frac{\pm x}{a}\right) = \left(\frac{x}{a}\right) = \left(\frac{a}{x}\right)$$

puisque a est de la forme $4k+1$.

Si ensuite a n'est pas premier, on aura $a = bc$ et b et c seront tous les deux de la forme $4k+1$ ou tous les deux de la forme $4k+3$.

Dans le premier cas, on aura

$$\left(\frac{a}{2na \pm x}\right) = \left(\frac{b}{2na \pm x}\right)\left(\frac{c}{2na \pm x}\right) = \left(\frac{b}{x}\right)\left(\frac{c}{x}\right) = \left(\frac{bc}{x}\right) = \frac{a}{x}.$$

Dans le second cas, il vient

$$\left(\frac{a}{2na \pm x}\right) = \left(\frac{b}{2na \pm x}\right)\left(\frac{c}{2na \pm x}\right) = \pm\left(\frac{2na \pm x}{b}\right) \cdot \pm\left(\frac{2na \pm x}{c}\right)$$
$$= \pm\left(\frac{x}{b}\right) \cdot \pm \frac{x}{c}.$$

Le signe du caractère dans le deuxième membre dépend de la nature du nombre premier $2na \pm x$. De toute façon, on aura le même signe pour les deux facteurs, donc le signe $+$ pour leur produit.

Ainsi

$$\left(\frac{a}{2na + x}\right) = \left(\frac{x}{b}\right)\left(\frac{x}{c}\right) = +\left(\frac{b}{x}\right) \cdot +\left(\frac{c}{x}\right) = +\left(\frac{bc}{x}\right) = \frac{a}{x},$$

les signes de $\left(\frac{b}{x}\right)$ et $\left(\frac{c}{x}\right)$ devant encore être les mêmes.

Exemple. — 5 est résidu de tout nombre premier de la forme $10a \pm 1$:

$$\left(\frac{5}{10a \pm 1}\right) = +1.$$

On démontrera de la même façon les formules suivantes :

$$\left(\frac{a}{4na \pm x}\right) = \left(\frac{a}{x}\right),$$
$$\left(\frac{-a}{4na + x}\right) = \left(\frac{-a}{x}\right),$$
$$\left(\frac{-a}{2na + x}\right) = \left(\frac{-a}{x}\right)$$

si

$$a \equiv 3 \pmod 4.$$

Dans toutes ces formules, les quantités $4na \pm x$, $4na + x$, $2na + x$, ainsi que x sont supposés premiers, a est quelconque dans les deux premières formules et $\equiv 3 \pmod 4$ dans la quatrième, mais a est supposé être positif.

31. Revenons à la congruence symbolique

$$\left(\frac{a}{x}\right) = 1.$$

Supposons d'abord que a est positif.

Par les formules que nous venons d'établir

$$\left(\frac{a}{2na \pm x}\right) = \left(\frac{a}{x}\right), \qquad \left(\frac{a}{4na \pm x}\right) = \left(\frac{a}{x}\right),$$

dont la première s'applique au cas où a est de la forme $4k+1$, et dont la deuxième est vraie quel que soit a, on voit que les valeurs dont a est résidu forment des progressions dont la raison est $2a$, si a est de la forme $4k+1$ et $4a$ dans les autres cas. Il suffit donc de trouver tous les nombres inférieurs à $2a$ dans le premier cas, ou inférieurs à $4a$ dans le second cas, pour avoir le premier terme de ces progressions. Il suffit même de connaître la moitié de toutes ces valeurs, car on trouve l'autre moitié en soustrayant la moitié déjà trouvée de $2a$ ou de $4a$.

Bien entendu, il faut éliminer de ces progressions les nombres non premiers.

Exemples. — 1° $a = 5$. Pour trouver tous les nombres dont 5 est résidu, il suffit de trouver tous les nombres inférieurs à 10 dont 5 est résidu. Ces nombres sont 1.3.7 et 9, et 5 est résidu de 1 et de 9 (plus exactement, 5 est résidu de $10k+9$); donc, d'une façon générale, 5 sera résidu de $10k+1$ et de $10k+9$ ou de $10k \pm 1$. Ces deux formes linéaires donnent les deux progressions :

1.11.21.31.41.51.61.71.81.91.101...

9.19.29.39.49.59.69.79.89.99.109...

dont il faut éliminer les nombres composés pour avoir tous les nombres dont 5 est résidu.

On trouve

1.11.31.41.61.71.101.131...

19.29.59.79.89.109.139.149....

2° Considérons une valeur composée de a, par exemple

$$a = 33 = 3.11.$$

Pour trouver tous les nombres dont 33 est résidu, on écrira tous les $\varphi(33) = 20$ nombres inférieurs à 33 et premiers avec 33. Ce sont les nombres

$$1.2.3.4.5.7.8.10.13.14.16.17.19.20.23.25.26.28.29.31 \text{ et } 32$$

dont on peut supprimer les nombres pairs comme premiers avec $2 \times 33 = 66$.

Il reste les nombres

$$1.5.7.13.17.19.23.25.29.31.$$

Nous allons voir pour lesquels de ces nombres $33 = 3.11$ est résidu. Or, 33 ne peut être résidu que si 3 et 11 sont tous les deux résidus ou tous les deux non-résidus.

Si l'on désigne par r un résidu et par n un non-résidu, on trouve que pour

$N =$	1	5	7	13	17	19	23	25	29	31
$3 =$	r	n	n	r	n	n	r	r	n	n
$11 =$	r	r	r	n	n	r	n	r	n	n
$\left(\frac{33}{N}\right) =$	r				r			r	r	r

Ainsi 33 est résidu de a :

$$1 \quad 17 \quad 25 \quad 29 \quad 31$$

et de $66 - a$:

$$65 \quad 49 \quad 41 \quad 37 \quad 35$$

ou, d'une façon générale, de

$$66k \pm 1.17.25.29.31.$$

Remarque. — On ne peut pas supprimer la valeur $a = 25$, bien que 25 ne soit pas premier, mais $66k \pm 25$ peut devenir un nombre premier. Pour déterminer le caractère de 3 (mod 25), on cherchera le caractère de 3 (mod $66k + 25$).

On trouve

$$\left(\frac{3}{66k + 25}\right) = \left(\frac{66k + 25}{3}\right) = \left(\frac{1}{3}\right) = +1.$$

3° Prenons $a = 3$. Cette fois-ci la raison de la progression est $4 \times 3 = 12$. Les nombres inférieurs à 12 et premiers avec 12 sont

1.5.7.11. Or, 3 n'est résidu que de 1 et de 11; donc les nombres dont 3 est résidu sont $12k+1$ et $12k+11$, ou bien $12k\pm1$.

4° $a=7$; $4a=28$. Il suffit d'essayer les nombres impairs inférieurs à $28:2=14$ et premiers avec 14. On trouvera les autres en soustrayant de 28 les nombres trouvés.

Les nombres inférieurs à 14 et premiers avec 14 sont :

$N =$	1	3	5	9	11	13
$\left(\frac{7}{N}\right) =$	r	r	n	r	n	n

Donc 7 est résidu de $28n\pm1.3.9$.

5° Considérons, enfin, un nombre contenant plus de deux facteurs tels que $a=66=2.3.11$. Or, 66 ne peut être résidu d'un nombre que si tous les facteurs sont résidus, ou bien si un seul est résidu.

De plus, la raison de la progression est $4a=264$ et il suffit d'examiner tous les nombres inférieurs à $264:2=132$ et premiers avec 132. On aura $\varphi(132)=40$ nombres à examiner :

$N =$	1	5	7	13	17	19	23	25	29	31	35	37	41	43	47	49	53	59	61	65
$\left(\frac{2}{N}\right) =$	+		+		+		+	+		+			+		+	+				+
$\left(\frac{3}{N}\right) =$	+			+			+	+			+	+			+	+		+	+	
$\left(\frac{11}{N}\right) =$	+	+	+			+		+			+	+		+		+	+			
$\left(\frac{66}{N}\right) =$	+	+		+	+	+		+		+			+	+		+	+	+	+	+

$N =$	67	71	73	79	83	85	89	91	95	97	101	103	107	109	113	115	119	125	123	131
$\left(\frac{2}{N}\right) =$		+	+	+			+		+	+		+			+		+		+	
$\left(\frac{3}{N}\right) =$		+	+		+	+			+	+			+	+			+			+
$\left(\frac{11}{N}\right) =$				+	+		+		+	+			+		+			+	+	+
$\left(\frac{66}{N}\right) =$						+			+	+		+		+				+		

Ainsi 66 n'est résidu que des nombres suivants :

$264k + 1.5.13.17.19.25.31.41.43.49.53.59.61.65.85.95.97.103.109.125.$

Remarque. — On peut aussi décomposer 66 en deux facteurs tels que 2 et 33 ou 3 et 22 et opérer comme au deuxième exemple. Il faut alors posséder les solutions de $\left(\frac{33}{x}\right) = 1$ ou de $\left(\frac{22}{x}\right) = 1$.

32. Supposons maintenant que a soit négatif. La raison de la progression est alors $2a$ si $a \equiv 3 \pmod 4$ et $4a$ dans les autres cas.

Exemples. — 1° $a = -1$ est résidu de $4k + 1$.

2° $a = -2$. Si l'on examine les nombres $1.3.5.7$, on remarque que -2 n'est résidu que de 1 et 3; donc -2 est résidu de $8k + 1.3$.

3° $a \equiv -3$ est résidu de $6k + 1$.

4° $a \equiv -5$ est résidu de $20k + 1.3.7.9$.

5° $a \equiv -6$. Considérons tous les nombres inférieurs à

$$6 \times 24 = 24$$

et premiers avec 24 :

N =	1	5	7	11	13	17	19	23
$\left(\frac{2}{N}\right) =$	+		+			+		+
$\left(\frac{-3}{N}\right) =$	+		+		+		+	
$\left(\frac{-6}{N}\right) =$	+	+	+	+				

Il en résulte que -6 est résidu pour

$$N = 24k + 1.5.7.11.$$

6° $a \equiv -30$. On peut décomposer -30 en deux facteurs (-6) et $+5$ pour lesquels on connaît les formules linéaires.

Ainsi

(-6) est résidu pour $24k + 1.5.7.11$,

5 » $10k \pm 1$.

Or, pour que $a = -30$ soit résidu, il faut que les deux facteurs soient tous deux résidus ou tous deux non-résidus.

Tous les deux sont résidus pour

$$N = 120k + 1.11.29.31.49.59.79.101.$$

Ils sont tous les deux non-résidus pour

$$N = 120k + 13.17.23.37.43.47.67.113.$$

Donc $a = -30$ est résidu de

$$N = 120k + 1.11.13.17.23.29.31.37.43.47.49.59.67.79.101.113.$$

33. On trouve ainsi toujours la forme linéaire des nombres premiers pour lesquels $\pm a$ est résidu.

Ces formules linéaires sont très importantes pour la recherche des facteurs d'un nombre.

Si, par exemple, on trouve que $\pm a$ est résidu d'un nombre à factoriser, on est certain que $\pm a$ est résidu des facteurs de ce nombre, et partant ce facteur ne peut être que parmi ceux qui sont donnés par les formes linéaires correspondant au résidu $\pm a$.

A raison de l'importance de ces résultats, nous donnons une Table de solutions de

$$\left[\frac{\pm x}{a}\right] = 1$$

pour toutes les valeurs de a inférieures à 200.

Nous verrons dans la suite (V, **35**, **36**; VI, **2**) comment on trouve un résidu d'un nombre dont on ignore la nature (premier ou composé).

34. La théorie que nous venons d'exposer trouve son application dans la théorie des formes quadratiques. Tout en nous réservant de traiter ce sujet dans le deuxième Volume de cet Ouvrage, nous donnerons ici les premiers éléments de cette théorie.

Nous considérerons les formes quadratiques simples, telles que $x^2 \pm Dy^2$. Disons une fois pour toutes que x et y seront toujours supposés premiers entre eux. Dans le cas contraire, si x et y ont un diviseur commun d, l'expression $x^2 \pm Dy^2$ sera divisible par d^2, et ce facteur sera à écarter.

35. Théorème. — *Si le nombre N ou son multiple peut se représenter par la forme $x^2 \pm Dy^2$, le nombre $\mp D$ est résidu de N.*

En effet, si l'on a

$$x^2 \pm Dy^2 = N \text{ ou } KN,$$

on aura

$$x^2 \equiv \mp Dy^2 \pmod{N};$$

or x^2 et y^2 sont résidus (mod N), donc $\mp D$ est aussi résidu.

36. Le théorème que nous venons de démontrer est très important, car il permet de trouver les résidus des nombres dont on ignore la nature. Si l'on trouve plusieurs représentations quadratiques du nombre N, on aura plusieurs résidus $\pm D$, et, partant, plusieurs formes linéaires des diviseurs éventuels du nombre N.

Il reste à trouver les représentations quadratiques du nombre considéré.

Ce travail sera facilité par les quelques théorèmes que nous allons exposer.

37. Théorème. — *Les diviseurs linéaires de la forme quadratique $x^2 \pm Dy^2$ sont les mêmes que ceux de la forme $t^2 \pm D$.*

En effet, soit z l'associé de y (mod N) (II, 12). On aura donc

$$zy \equiv 1 \pmod{N}.$$

Or, si l'on multiplie $KN = x^2 \pm Dy^2$ par z, il vient

$$zKN = z^2x^2 + Dy^2z^2 \quad \text{ou} \quad zKN = (xz)^2 + D$$

ou

$$(xz)^2 \pm D \equiv 0 \pmod{N} \quad \text{ou} \quad t^2 \pm D \equiv 0 \pmod{N}$$

étant posé $xz \equiv t$ (mod N).

Il s'ensuit que si N ou son multiple peut être représenté par la forme $x^2 \pm Dy^2$, ce même nombre ou son multiple peut également être représenté par $t^2 \pm D$. Inversement, tout nombre N qui divise $t^2 \pm D$ divise aussi $x^2 \pm Dy^2$.

38. Théorème. — *Tout nombre qui divise une somme de deux carrés est également une somme de deux carrés.*

Soit p un nombre qui divise une somme de deux carrés x^2+y^2, le même nombre p divise aussi une somme de deux carrés x^2+1 (IV, 37). On aura donc

$$x^2+1\equiv 0 \pmod p.$$

Exprimons maintenant $\frac{x}{p}$ en fraction continue et cherchons toutes les réduites dont la dernière est $\frac{x}{p}$. Comme les dénominateurs des réduites croissent de 1 à p, on trouvera toujours deux réduites successives

$$\frac{p_n}{q_n} \quad \text{et} \quad \frac{p_{n+1}}{q_{n+1}}$$

telles que

$$q_n^2 < p < q_{n+1}^2.$$

Cela étant, on aura

$$\left(\frac{x}{p}-\frac{p_n}{q_n}\right)^2 < \frac{1}{q_n^2 q_{n+1}^2} \qquad \text{ou} \qquad (xq_n - pp_n)^2 < \frac{p^2}{q_{n+1}^2} < p$$

ou, si l'on ajoute q_n^2 aux deux membres, il vient

$$(xq_n - pp_n)^2 + q_n^2 < p + q_n^2 < 2p$$

ou bien

$$(x^2+1)q_n^2 - 2pxp_nq_n + p^2p_n^2 < 2p.$$

Or, le premier membre de cette inégalité est positif et un multiple de p, donc on aura

$$(xq_n - pp_n)^2 + q_n^2 = p,$$

c'est-à-dire que p est une somme de deux carrés.

39. Théorème. — *Tout nombre premier de la forme $4k+1$ est une somme de deux carrés.*

En effet, nous avons vu (III, 10) que tout nombre premier de la forme $4k+1$ divise une somme de deux carrés

$$[1.2.3\ldots(2k)]^2+1,$$

et puisque tout diviseur d'une somme de deux carrés est une somme de deux carrés, ce nombre $4k+1$ est une somme de deux carrés.



40. Ainsi que nous l'avons vu (V, 39), tout nombre premier de la forme $4k+1$ est une somme de deux carrés. Pour ce qui est des nombres premiers de la forme $4k+3$, ils ne sont jamais une somme de deux carrés, car si $N = x^2+y^2$, (-1) est résidu de N; or (-1) n'est pas résidu d'un nombre de la forme $4k+3$.

Voyons maintenant comment se comporteront les nombres composés;

Si N est composé et est de la forme $4k+3$, il contient un facteur (ou en général un nombre impair) de la forme $4k+3$ et ne peut pas devenir une somme de deux carrés, car, dans le cas contraire, ce nombre composé N admettrait des diviseurs $4k+3$ qui ne sont pas sommes de deux carrés, ce qui est contraire au théorème du paragraphe 38.

Pour les nombres composés de la forme $4k+1$, il y a deux cas à considérer :

1° Si le nombre composé $N=4k+1$ contient deux facteurs (ou en général un nombre pair) de la forme $4k+3$, la décomposition en sommes de deux carrés est impossible;

2° Si le nombre composé N ne contient que des facteurs de la forme $4k+1$, la décomposition en sommes de deux carrés est possible de plusieurs manières, comme nous allons le voir.

41. Soit donc un nombre N composé de n facteurs inégaux

$$N = a_1 a_2 a_3 \ldots a_n,$$

chacun de la forme $4k+1$. Voyons comment se fera la décomposition de N en sommes de deux carrés.

On a

$$(a^2+b^2)(c^2+d^2) = (ac \pm bd)^2 + (ad \mp bc)^2,$$

identité (Euler) qui prouve que le produit de deux nombres, dont chacun est une somme de deux carrés, est aussi une somme de deux carrés de deux façons différentes.

On aura donc autant de façons différentes de décomposer N en sommes de deux carrés, qu'il y a de façons différentes de décomposer N en deux facteurs.

Or, on peut décomposer N en deux facteurs de la manière suivante :

On prendra

1	pour 1 facteur et	N	pour l'autre, d'où	1	solution
a_i	»	$\frac{N}{a_i}$	»	n	»
$a_i a_k$	»	$\frac{N}{a_i a_k}$	»	C_n^2	»
3 facteurs	»	$(n-3)$ restants	»	C_n^3	»
.....	.....	.....	.....	.....	.....
N	»	1	»	1	»

C_n^i désignant le nombre de combinaisons de n lettres pris i à i.

Or, la somme

$$1+n+C_n^2+C_n^3+\ldots+1=C_n^0+C_n^1+C_n^2+\ldots+C_n^n=2^n.$$

[On s'en assure en prenant le développement par la formule du binome de $(1+1)^n$.]

Puisque nous avons compté chaque décomposition de N deux fois, le nombre de décompositions du nombre N en deux facteurs est $2^n : 2 = 2^{n-1}$. Le nombre de décompositions en somme de deux carrés est aussi 2^{n-1} (I, 14).

Exemple. — $32045 = 5.13.17.29$ est un produit de quatre facteurs et peut être représenté par une somme de deux carrés de $2^3 = 8$ façons différentes.

Voici les huit solutions de $N = 32045 = x^2 + y^2$:

$$\begin{array}{lcccccccc} x = & 2 & 46 & 74 & 86 & 122 & 143 & 166 & 178, \\ y = & 179 & 173 & 163 & 157 & 131 & 109 & 67 & 19. \end{array}$$

42. En pratique, la question se présente d'une autre façon.

Soit N un nombre dont on ignore la nature. Supposons que N soit de la forme $4k+1$. On est alors amené à chercher la décomposition de N en x^2+y^2.

On ne trouvera qu'une solution si N est premier, on n'en trouvera aucune si N est composé et contient deux facteurs (ou en général un nombre pair) de la forme $4k+3$. Enfin, on trouvera plusieurs solutions si N est composé de facteurs de la forme $4k+1$.

On verra, dans la suite, comment on trouve alors les facteurs.

43. On peut répéter à peu près la même chose que ce que nous avons développé pour la forme x^2+y^2 pour les formes x^2+2y^2 et x^2+3y^2.

Nous abrégeons et résumons les conclusions :

1° Tout diviseur de x^2+2y^2 est aussi de la forme t^2+2u^2.

2° Tout diviseur de x^2+3y^2 est aussi de la forme t^2+3u^2.

3° Tout nombre premier de la forme $8k+1.3$ peut être mis sous la forme x^2+2y^2, et cela d'une seule façon.

4° Tout nombre premier de la forme $6k+1$ peut être mis sous la forme x^2+3y^2, et cela d'une seule manière.

5° Les nombres composés de la forme $8k+1.3$ ne peuvent être mis sous la forme x^2+2y^2 que s'ils ne contiennent pas d'autres facteurs que ceux de la forme linéaire précitée.

6° Les nombres composés de la forme $6k+1$ peuvent être mis sous la forme x^2+3y^2 s'ils contiennent uniquement les facteurs de la forme $6k+1$.

7° Pour un nombre composé de n facteurs convenables, on aura 2^{n-1} décompositions différentes.

Voici comment on démontre les deux premières propositions :

Si p divise x^2+2y^2, p divise aussi x^2+2 (IV, 37) et l'on aura

$$x^2+2\equiv 0 \pmod{p}.$$

Soit $\frac{p_n}{q_n}$ la réduite choisie comme il est dit (IV, 38). On aura, comme dans le paragraphe cité,

$$(xq_n-pp_n)^2+2q_n^2<p+2q_n^2<3p,$$

et puisque le premier membre de cette inégalité est $\equiv 0 \pmod{p}$, le deuxième membre ne peut être que p ou $2p$.

On aura donc

$$(xq_n-pp_n)^2+2q_n^2=p, \qquad \text{c'est-à-dire} \qquad p=z^2+2y^2,$$

ou bien

$$(xq_n-pp_n)^2+2q_n^2=2p \qquad \text{et} \qquad p=2\left(\frac{xq_n-pp_n}{2}\right)^2+q_n^2=2z^2+y^2.$$

De même, si p est diviseur de x^2+3y^2, p divisera aussi x^2+3 (IV, 37) et, en choisissant p_n et q_n comme précédemment, on aura

$$(xq_n - pp_n)^2 + 3q_n^2 < p + 3q_n^2 < 4p.$$

Le premier membre étant divisible par p, le second ne peut être que p, $2p$ ou $3p$.

Donc

$$(xq_n - pp_n)^2 + 3q_n^2 = p, \quad 2p \text{ ou } 3p.$$

Or l'égalité

$$(xq_n - pp_n)^2 + 3q_n^2 = 2p$$

est impossible, car p étant diviseur de x^2+3y^2 est de la forme $6k+1$ et

$$(xq_n - pp_n)^2 + 3q_n^2 = 2p$$

deviendrait

$$(0 \text{ ou } 1) + (0 \text{ ou } 3) \equiv 2 \pmod 4,$$

ce qui est impossible.

On aura donc

$$(xq_n - pp_n)^2 + 3q_n^2 = p \text{ ou } 3p.$$

Dans le premier cas,

$$p = z^2 + 3y^2;$$

dans le second cas, on aura

$$p = 3\left(\frac{xq_n - pp_n}{3}\right)^2 + q_n^2 = 3z^2 + y^2,$$

ce qui est de la même forme.

Les autres propositions se démontrent comme pour le cas de x^2+y^2.

On remarquera l'identité

$$(x^2 + Dy^2)(z^2 + Dt^2) = (xz \pm Dyt)^2 + D(xt \mp yz)^2,$$

analogue à celle d'Euler (IV, 41).

44. Il nous reste à montrer l'application de la théorie des résidus quadratiques à la résolution des équations indéterminées.

Nous considérerons le cas d'une équation à deux inconnues. Si l'on a n équations à $(n+1)$ inconnues, on éliminera toutes

les inconnues, sauf deux, et l'on entrera dans le cas que nous allons envisager.

Nous étudierons successivement les équations

$$ax + by + c = 0, \qquad axy + bx + cy + d = 0, \qquad ax^2 + bx + c = y^2,$$
$$x^2 + Dy^2 = N,$$

et d'une façon générale l'équation

$$f(x) = F(x),$$

f et F étant des fonctions algébriques.

Il est entendu que nous nous bornerons aux solutions entières et, s'il n'y en a pas, nous dirons que l'équation est impossible.

45. L'équation $ax + by + c = 0$ n'est mentionnée ici que pour compléter l'ensemble. Elle fait l'objet de l'Algèbre élémentaire; d'ailleurs elle se ramène à une congruence du premier degré, toujours possible si a et b sont premiers entre eux.

On sait que l'équation $ax + by = c$ admet à une unité près

$$n = E\left(\frac{c}{ab}\right)$$

solutions entières et positives, $E(x)$ désignant le plus grand entier contenu dans x.

Si a et b sont de signe contraire, l'équation $ax - by = c$ admet une infinité de solutions entières et positives.

46. Considérons l'équation bilinéaire

$$axy + bx + cy + d = 0.$$

Si l'on prend pour inconnue xy et $bx + cy$, on aura une équation linéaire en xy et $(bx + cy)$ qui admet des solutions telles que

$$xy = r_1,$$
$$bx + cy \equiv r_2 \pmod{a},$$

ou, t étant une nouvelle inconnue,

$$bx + cy = at + r_2,$$
$$xy = -t + r_1.$$

d'où

$$(at + r_2)^2 - 4bc(-t + r_1) = z^2,$$

ce qui nous ramène à une équation du second degré

$$A^2t^2 + 2Bt + C = z^2,$$

dont nous allons nous occuper.

47. Soit l'équation

$$ax^2 + bx + c = y^2.$$

Sans nous arrêter aux solutions qu'on ne peut obtenir que dans le cas où l'on peut factoriser le nombre $b^2 - 4ac$, nous allons exposer la méthode qui donne la solution, entre les limites assignées, dans tous les cas.

Supposons qu'il s'agisse de déterminer une solution entre les limites l_1 et l_2 de l'équation

$$ax^2 + bx + c = y^2.$$

On prendra pour module m les nombres 2 ou 2^n, 3 ou 3^n, 5 ou 5^n, 7.11.13.17...; on donnera à x toutes les valeurs possibles pour ce module :

$$x \equiv 0.1.2.3\ldots(m-1) \pmod{m}.$$

On calculera la valeur de $y^2 = ax^2 + bx + c$ et l'on formera le tableau

$$x \equiv 0.1.2.3.4\ldots(m-1) \pmod{m},$$
$$y^2 \equiv b_1 b_2 b_3 b_4 \ldots b_m \pmod{m}.$$

Or il se fait que certaines valeurs b_i sont résidus $(\text{mod}\, m)$, certaines autres non-résidus $(\text{mod}\, m)$.

Si une certaine valeur x conduit à un non-résidu, cette valeur de x est à éliminer.

On forme ainsi une suite de formes linéaires qui contribuent à l'élimination de valeurs non convenables de x.

Si, par le procédé que nous avons indiqué (II, 18-20), on crible toutes les valeurs entre les limites assignées, on trouvera toutes les solutions qui se trouvent entre ces limites.

Exemple. — L'étude du nombre $N = 649\,301\,712\,182\,209$ nous a conduit à l'équation

$$21\,316 x^2 + 25\,620\,081 x + 83\,116\,418 = y^2$$

avec des limites

$$-3 < x < 71\,628.$$

(*Voir* pour les détails le numéro spécial de *Sphinx Œdipe*, p. 13-16; Nancy, 1911. Le nombre N est un facteur de $2^{73} + 2^{37} + 1$ qui est lui-même facteur de $2^{146} + 1$.)

On trouve les formes linéaires suivantes :

Modules.	Formes linéaires.
16	2.3.11.14
9	5.7
25	2.7.12.13.17.21.22
7	0.3.4.6
11	0.1.2.5.6.7
13	1.2.3.5.6.7
17	0.1.2.3,4.5.8.14
...	...

On ne trouve aucune solution entre les limites assignées.

Comme cas particulier de l'équation générale

$$ax^2 + bx + c = y^2,$$

on obtient pour $a = 0$ l'équation $y^2 = bx + c$, qui ne diffère que par la notation de celle que nous avons étudiée (IV, **24-25**).

48. Considérons ensuite l'équation générale $f(x) = F(y)$ dont toutes celles que nous avons envisagées ne sont qu'un cas particulier.

Si, en général, les polynomes $f(x)$ et $F(y)$ sont quelconques, on procédera de la façon suivante :

On cherchera la valeur de $f(x)$ et de $F(y)$ pour un système complet de valeurs de x ou y (mod m) :

$$x \text{ ou } y \equiv 0.1.2.3\ldots(m-1) \pmod{m},$$
$$f(x) \equiv b_1\, b_2 \ldots b_m,$$
$$F(y) \equiv c_1\, c_2 \ldots c_m.$$

Si, pour $x = i$, la valeur correspondante de $F(y) = c_{i+1}$ ne figure pas parmi celles qu'on obtient pour $f(x)$, c'est-à-dire parmi les b, la valeur $x \equiv i \pmod{m}$ est inadmissible.

On obtiendra donc une série de formes linéaires de x, et par le procédé que nous avons indiqué (III, 17-21) on trouvera les solutions.

Il est toutefois à noter que le procédé est inapplicable quand les deux fonctions sont linéaires. Mais alors l'équation donnée n'est que du premier degré et admet une solution directe.

Il y a une précaution à prendre : Si les degrés des polynomes sont respectivement m et n, il est bon de n'employer comme module des nombres premiers p, de sorte que $p - 1$ soit divisible par le plus petit commun multiple de m et n.

Si, par conséquent, les deux polynomes sont du deuxième degré, tout nombre premier peut être pris pour module. Mais si un des polynomes est du troisième degré, par exemple $F(y) = y^3$, il est clair que, pour un module de la forme $6k + 5$, $F(y)$ peut prendre toutes les valeurs possibles. On utilise, dans ce cas, les modules de la forme $6k + 1$. A cet effet, on trouvera une Table de résidus à la fin de ce Volume (Table IV).

49. Les équations de la forme $x^2 + Dy^2 = N$ entrent dans le cas envisagé. Une attention toute spéciale doit être apportée aux formes suivantes :

$$x^2 - y^2 = N,$$

$$x^2 + y^2 = N, \qquad x^2 + 2y^2 = N, \qquad x^2 + 3y^2 = N.$$

L'importance de la première est évidente. Si l'on parvient à trouver une solution de $N = x^2 - y^2$, on aura la factorisation de N. Si, au contraire, on connaît la décomposition de N, on aura une solution en décomposant N en deux facteurs et en prenant un des facteurs (le plus grand) pour $x + y$, et l'autre pour $x - y$. Il y aura évidemment 2^{n-1} solutions, n étant le nombre de facteurs contenus dans N (IV, 41).

L'importance des autres équations sera montrée dans le deuxième Volume. On verra que les décompositions de N en $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$ servent pour reconnaître les caractères résiduels plus élevés.

Aussi donnons-nous une Table donnant les solutions de l'équation $x^2 + Dy^2 = N$.

Nous n'avons pas étudié l'équation

$$x^2 - Ay^2 = \pm 1 \quad \text{ou} \quad x^2 - Ay^2 = \mp D$$

qui admet une solution directe. Nous nous réservons de revenir, dans le deuxième Volume, sur ce très important sujet.

CHAPITRE V.

CONGRUENCES BINOMES. INDICES. CONGRUENCES EXPONENTIELLES.

1. Nous allons nous occuper des congruences de la forme

$$X^m \equiv A \pmod{p}.$$

Nous commencerons par le cas le plus simple. C'est le cas de $A = 1$ et quand p est un nombre premier. Nous allons d'abord démontrer la proposition suivante :

Théorème. — *Si le même nombre $x = r \pmod{p}$ satisfait à deux congruences*

$$x^m \equiv 1 \quad \text{et} \quad x^n \equiv 1,$$

il satisfait aussi à la congruence $x^d \equiv 1 \pmod{p}$, d étant le plus grand commun diviseur de m et n.

En effet, d étant le plus grand commun diviseur de m et n, $m = dy$, $n = dz$ avec y et z premiers entre eux.

Or, y et z étant premiers entre eux, on peut trouver deux nombres u et v tels que $yu - zv = 1$, ce qui donne, en multipliant par d,

$$dyu - dzv = d \quad \text{ou} \quad mu - nv = d.$$

Puisque $r^m \equiv r^n \equiv 1 \pmod{p}$, on aura aussi

$$r^{mu} \equiv r^{nv} \equiv r^{mu-nv} \equiv r^d \equiv 1 \pmod{p}.$$

2. Théorème. — *Si m est la plus petite puissance de a qui est $\equiv 1 \pmod{p}$, m est diviseur de $p-1$.*

En effet, on aura par hypothèse $a^m \equiv 1 \pmod{p}$ et, puisque (III, 1) $a^{p-1} \equiv 1 \pmod{p}$, on aura aussi (V, 1) $a^d \equiv 1 \pmod{p}$, d étant le plus grand commun diviseur de m et $p-1$. Or, m est

la plus petite puissance de a qui est $\equiv 1 \pmod{p}$; donc d n'est pas inférieur à m. Comme m n'est divisible par aucun nombre plus grand que m, on aura $d = m$; m est donc un diviseur de $p-1$.

3. Théorème. — *d désignant le plus grand commun diviseur de m et de $p-1$, la congruence $x^m \equiv 1 \pmod{p}$ admet d solutions qu'on peut obtenir de la congruence $x^d \equiv 1 \pmod{p}$.*

En effet (V, 1), toute solution de la congruence $x^m \equiv 1 \pmod{p}$ est aussi une solution de la congruence $x^d \equiv 1 \pmod{p}$. La deuxième partie de la proposition est donc établie. Reste à démontrer que la congruence $x^d \equiv 1 \pmod{p}$ admet d solutions.

On sait (III, 14, 15) que la congruence $x^d \equiv 1 \pmod{p}$ admet d solutions, si tous les coefficients du reste de la division de $x^p - x$ par $x^d - 1$ sont $\equiv 0 \pmod{p}$.

Or, $x^p - x = x(x^{p-1} - 1)$; de plus, d étant diviseur de $p-1$, $x^{p-1} - 1$ est divisible par $x^d - 1$, donc $x^p - x$ est divisible par $x^d - 1$, donc la congruence $x^d \equiv 1 \pmod{p}$ admet réellement d solutions.

4. Théorème. — *La congruence $x^m \equiv 1 \pmod{p}$, m étant un diviseur de $p-1$, peut être satisfaite par $x \equiv k^n$, k étant premier avec p et n le quotient de la division de $p-1$ par m, $p-1 = mn$.*

En effet,

$$a^m \equiv k^{mn} \equiv k^{p-1} \equiv 1 \pmod{p}.$$

5. Théorème. — *Si $x \equiv r \pmod{p}$ satisfait à la congruence $x^m \equiv 1 \pmod{p}$ sans satisfaire aux congruences*

$$x^a \equiv 1 \quad \text{et} \quad x^b \equiv 1, \quad \ldots \pmod{m},$$

a, b, ... étant les différents diviseurs de m (en y comprenant aussi le nombre 1), toutes les m solutions de la congruence $x^m \equiv 1$ seront

$$x \equiv r, \quad x \equiv r^2, \quad x \equiv r^3, \quad \ldots, \quad x \equiv r^m \pmod{p}.$$

[La dernière solution donne $x \equiv r^m \equiv 1$ qui est aussi solution de

$x^m \equiv 1 \pmod p$, mais satisfait à une congruence $x^a \equiv 1 \pmod p$ avec $a = 1$.]

Remarquons d'abord que si $x \equiv r \pmod p$ est solution de la congruence $x^m \equiv 1 \pmod p$, toute puissance de r est aussi une solution, car $x = r^n$ donnerait

$$x^m \equiv r^{nm} \equiv r^{mn} \equiv 1^n \equiv 1 \pmod p.$$

Ainsi les nombres

$$x \equiv r, \quad x \equiv r^2, \quad \ldots, \quad x = r^m \pmod p$$

satisfont tous à la congruence $x^m \equiv 1 \pmod p$.

Et si nous parvenons à établir qu'ils sont tous différents, le théorème sera démontré.

Or, supposons, au contraire, que deux puissances telles que

$$x \equiv r^h \quad \text{et} \quad x \equiv r^k \pmod p$$

soient identiques, h et k étant tous les deux compris entre 0 et m et $h > k$.

On aura donc

$$r^h \equiv r^k \quad \text{ou} \quad r^{h-k} \equiv 1 \pmod m,$$

ce qui est contraire à l'hypothèse, car r serait alors solution de la congruence $x^{h-k} \equiv 1 \pmod p$, donc aussi de la congruence $x^d \equiv 1 \pmod p$, d étant le plus grand commun diviseur de $h - k$ et m, donc inférieur à m, puisque $h - k$ est évidemment inférieur à m.

Ainsi les nombres

$$x \equiv r, \quad x \equiv r^2, \quad \ldots, \quad x \equiv r^m \pmod p$$

sont tous différents, et sont tous solutions de la congruence donnée $x^m \equiv 1 \pmod p$. Ils constituent donc un système complet de solutions.

6. Ainsi, parmi les solutions de la congruence $x^m \equiv 1 \pmod p$, il y a des solutions qui satisfont à la congruence donnée sans satisfaire à une congruence de même espèce, mais avec un plus petit exposant. Il y a d'autres solutions qui satisfont à la congruence donnée, mais satisfont aussi à une congruence de même espèce

dont l'exposant est un diviseur de m. Une solution de la première espèce sera dite « racine primitive de la congruence donnée ». Il convient de ne pas confondre la racine primitive d'une congruence avec une racine primitive d'un nombre dont il sera question ultérieurement.

Ainsi la congruence $x^6 \equiv 1 \pmod{19}$ admet six solutions :

$$x \equiv 1.7.8.11.12.18 \pmod{19};$$

de ces six solutions, la première est aussi solution de la congruence $x^1 \equiv 1 \pmod{19}$, la dernière est solution de $x^2 \equiv 1 \pmod{19}$; les solutions $x \equiv 7.11 \pmod{19}$ sont solutions de la congruence $x^3 \equiv 1 \pmod{19}$. Seules les solutions $x \equiv 8.12 \pmod{19}$ appartiennent à la congruence $x^6 \equiv 1 \pmod{19}$ sans satisfaire à $x^m \equiv 1 \pmod{19}$ avec $m = 1.2.3$.

Les seules racines primitives de la congruence $x^6 \equiv \pmod{19}$ sont 8 et 12 et toutes les autres solutions peuvent être obtenues moyennant l'une de ces solutions. Ainsi la solution $x \equiv 8 \pmod{19}$ donnerait

$$x \equiv 8, \quad x \equiv 8^2 \equiv 7, \quad x \equiv 8^3 \equiv 18, \quad x \equiv 8^4 \equiv 11, \quad x \equiv 8^5 \equiv 12,$$
$$x \equiv 8^6 \equiv 1 \pmod{19}.$$

De même la solution $x \equiv 12 \pmod{19}$ donnerait

$$x \equiv 12, \quad x \equiv 12^2 \equiv 11, \quad x \equiv 12^3 \equiv 18, \quad x \equiv 12^4 \equiv 7,$$
$$x \equiv 12^5 \equiv 8, \quad x \equiv 12^6 \equiv 1 \pmod{19},$$

ce qui donne, à l'ordre près, les six mêmes solutions.

7. Si l'on fait $m = p - 1$, on aura la congruence

$$x^{p-1} \equiv 1 \pmod{p}$$

qui admet $p - 1$ solutions

$$x \equiv 1.2.3\ldots(p-1) \pmod{p}.$$

La congruence donnée est donc vérifiée par n'importe quel nombre, les multiples de p ou les nombres qui sont $\equiv 0 \pmod{p}$ seuls devant être exceptés, car $x \equiv 0 \pmod{p}$ donnerait

$$x^{p-1} \equiv 0 \quad \text{et non} \quad \equiv 1 \pmod{p}.$$

Or, p étant supposé premier, $p-1$ est composé.

Soient d_1, d_2, d_3, ..., d_n tous les diviseurs de $p-1$, le nombre 1 étant compté parmi les diviseurs et n étant le nombre de diviseurs.

Les $(p-1)$ solutions de la congruence $x^{p-1} \equiv 1 \pmod{p}$ peuvent être distribuées en n groupes contenant chacun un nombre variable de termes.

1° Le premier groupe comprendra les nombres qui satisfont à la congruence $x^{d_1} \equiv 1 \pmod{p}$, d_1 étant le plus petit diviseur de $p-1$, donc $d_1 = 1$. Le seul nombre qui satisfait à la congruence $x^1 \equiv 1 \pmod{p}$ est $x \equiv 1 \pmod{p}$. Ainsi le premier groupe comprendra toujours le seul nombre 1.

2° Le deuxième groupe comprendra les nombres qui satisfont à la congruence $x^{d_2} \equiv 1 \pmod{p}$ sans satisfaire à la précédente $x^{d_1} \equiv 1 \pmod{p}$, d_2 étant le plus petit diviseur de $p-1$ en exceptant le diviseur d_1. Puisque p est supposé premier impair, on aura toujours $d_2 = 2$, car $p-1$ est évidemment pair.

Or, les solutions de la congruence $x^2 \equiv 1 \pmod{p}$ sont évidemment

$$x \equiv \pm 1 \pmod{p} \qquad \text{ou} \qquad x \equiv 1 \text{ ou } p-1 \pmod{p}.$$

De ces deux solutions, la première appartient à la congruence plus simple $x^1 \equiv 1 \pmod{p}$, la seconde est une solution primitive de la congruence $x^2 \equiv 1 \pmod{p}$.

3° Le troisième groupe comprendra les nombres qui satisfont à la congruence $x^{d_3} \equiv 1 \pmod{p}$ sans satisfaire à une congruence de même espèce, mais plus simple, d_3 étant le plus petit diviseur de $p-1$, sans compter les diviseurs d_1 et d_2 déjà examinés.

Il est facile de constater que cette congruence aura $\varphi(d_3)$ racines primitives. En effet, elle admet en tout d_3 solutions qui sont toutes primitives, sauf celles qui sont solutions de congruences de même espèce, mais plus simples.

En effet, d_3 est toujours divisible par 1, le nombre 1 étant compté parmi les diviseurs, donc une de ces d_3 solutions n'est pas racine primitive. Si maintenant d_3 est pair, une autre solution

$(x \equiv p - 1)$ n'est pas primitive non plus. Alors $d_3 = 4$, 4 étant le plus petit nombre pair en exceptant 2.

Or $\varphi(4) = 2$ et des quatre solutions de la congruence

$$x^4 \equiv 1 \pmod{p}$$

deux appartiennent aux congruences $x^1 \equiv 1$ et $x^2 \equiv 1 \pmod{p}$. Il ne restera donc que $4 - 2 = 2$ racines primitives de la congruence $x^4 \equiv 1 \pmod{p}$.

Si d_3 est impair, d_3 est nécessairement premier et

$$\varphi(d_3) = d_3 - 1.$$

Or, des d_3 solutions de la congruence $x^{d_3} \equiv 1 \pmod{p}$, une seule n'est pas primitive. Le nombre de solutions primitives est donc dans tous les cas $\varphi(d_3)$.

4° Soient enfin d_i un diviseur quelconque de $p - 1$ et e_1, e_2, e_3, ..., e_k tous les diviseurs de d_i (le nombre 1 est compté parmi les diviseurs); donc $e_1 = 1$, $e_k = d_i$.

On a

$$\varphi(e_1) + \varphi(e_2) + \ldots + \varphi(e_k) = d_i \qquad \text{(I, 19)}.$$

Or, des d_i solutions de la congruence $x^{d_i} \equiv 1 \pmod{p}$,

$\varphi(1) = 1$	solution appartient à la congruence	$x^1 \equiv 1$	$(\text{mod } p)$,
$\varphi(e_2) = \varphi(2) = 1$	»	$x^2 \equiv 1$	»
....	....	....	....
$\varphi(e_k)$	»	$x^k \equiv 1$	»

ce qui prouve que la congruence $x^{d_i} \equiv 1 \pmod{p}$ aura $\varphi(d_i)$ solutions primitives.

Ainsi la congruence $x^{p-1} \equiv 1 \pmod{p}$ aura $\varphi(p - 1)$ solutions primitives.

Si de plus

$$d_1 = 1, \qquad d_2 = 2, \qquad d_3, d_4, \ldots, d_n = p - 1$$

sont tous les diviseurs de $p - 1$, ces $p - 1$ solutions se répartissent de la façon suivante :

Solutions primitives.		Congruence.	
$\varphi(1) \equiv 1$	appartiennent à	$x^1 \equiv 1$	$(\bmod p)$
$\varphi(2) \equiv 1$	»	$x^2 \equiv 1$	»
$\varphi(d_3)$	»	$x^{d3} \equiv 1$	»
....			
$\varphi(d_i)$	»	$x^{d_i} \equiv 1$	»
....			
$\varphi(d_n) = \varphi(p-1)$	»	$x^{p-1} \equiv 1$	»

Ce sont les solutions primitives de la congruence $x^{p-1} \equiv 1 \pmod p$ qu'on appelle « racines primitives du nombre premier p ». (*Voir* V, 23, Exemple.)

8. Nous avons vu (V, 5) que si $x \equiv r \pmod p$ est une racine primitive d'une congruence $x^m \equiv 1 \pmod p$, toutes les racines de cette congruence s'obtiennent par les m puissances successives de r qui sont toutes distinctes.

Donc si r est une racine primitive du nombre p, c'est-à-dire une racine primitive de la congruence

$$x^{p-1} \equiv 1 \pmod p,$$

les $p-1$ puissances successives de r seront toutes différentes.

Il en résulte que la congruence

$$r^x \equiv a \pmod p$$

est toujours possible, sauf quand $a \equiv 0 \pmod p$, si r est une racine primitive de p. De plus, elle n'admet qu'une solution, inférieure à $p-1$.

On appelle x l'indice de $a \pmod p$ dans le système de base r.

Puisque $r^{p-1} \equiv 1$, l'indice n'est déterminé qu'à un multiple de $(p-1)$ près, car

$$r^x \equiv r^{x+k(p-1)} \equiv a,$$

ce qui montre que l'indice de a peut être indifféremment x ou $x+k(p-1)$. Nous pouvons donc écrire d'une façon générale

$$\text{indice } a \equiv x \pmod{p-1}$$

ou, en abrégé,

$$\text{ind } a \equiv x \pmod{p-1}.$$

9. Nous avons vu (V, 7) que tout nombre premier p aura $\varphi(p-1)$ racines primitives, ce qui donne $\varphi(p-1)$ systèmes d'indices pour chaque nombre premier p. Il est, toutefois, sans importance de se servir de tel ou tel système d'indices. Nous verrons du reste qu'on peut facilement passer d'un système d'indices à un autre.

Mais quelle que soit la base, on aura toujours

$$\operatorname{ind} 1 \equiv 0 \pmod{p-1},$$
$$\operatorname{ind}(p-1) \equiv \frac{p-1}{2}.$$

En effet, on a

$$r^0 \equiv r^{k(p-1)} \equiv 1 \pmod{p}$$

et

$$r^{\frac{p-1}{2}} \equiv -1 \equiv p-1.$$

La première relation est évidente. Pour ce qui est de la deuxième, remarquons qu'on a

$$r^{p-1} \equiv 1, \qquad \text{d'où} \qquad r^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Or, on ne peut pas avoir

$$r^{\frac{p-1}{2}} \equiv +1 \pmod{p},$$

car r ne serait pas alors racine primitive; donc

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Il importe de remarquer que le module est toujours p pour les nombres et $p-1$ pour les indices.

10. Théorème. — *L'indice d'un produit est égal à la somme des indices des facteurs; l'indice d'une puissance est égal au produit de l'indice de la base par l'exposant de la puissance.*

Soient

$$A \equiv r^a, \qquad B \equiv r^b, \qquad C \equiv r^c \pmod{p}$$

ou, ce qui revient au même,

$$a \equiv \operatorname{ind} A, \qquad b \equiv \operatorname{ind} B, \qquad c \equiv \operatorname{ind} C \pmod{p-1}.$$

On aura

$$ABC \equiv r^{a+b+c} \pmod{p}$$

ou

$$a + b + c \equiv \text{ind}(ABC) \pmod{p-1},$$

ou encore

$$\text{ind}(ABC) = \text{ind}\,A + \text{ind}\,B + \text{ind}\,C \pmod{p-1}.$$

De même, $A^m \equiv r^{am} \pmod{p}$ donne

$$\text{ind}(A^m) \equiv a^m \equiv m\,\text{ind}\,A \pmod{p-1}.$$

Corollaire. — L'indice d'un quotient $\frac{A}{B}$ est

$$\text{ind}\,A - \text{ind}\,B \pmod{p-1}.$$

En effet,

$$\frac{A}{B} = \frac{r^a}{r^b} = r^{a-b};$$

donc

$$\text{ind}\,\frac{A}{B} = a - b = \text{ind}\,A - \text{ind}\,B \pmod{p-1}.$$

11. Il résulte de ce qui précède qu'une Table d'indices peut rendre, dans la théorie des nombres, les mêmes avantages qu'une Table de logarithmes pour le calcul numérique.

La plus simple façon de construire une Table d'indices est de choisir une racine primitive, de préférence la plus petite ou 10 si cela est possible, et calculer la série complète de $p-1$ puissances de cette racine primitive.

Ainsi $p = 13$, $r = 2$ donneraient :

$x =$ 1	2	3	4	5	6	7	8	9	10	11	12	(mod 12),
$r^x =$ 2	4	8	3	6	12	11	9	5	10	7	1	(mod 13).

On aura ainsi :

ind 1 ≡ 12 ou 0, ind 2 ≡ 1, ind 3 ≡ 4, ind 4 ≡ 2, ind 5 ≡ 9,
ind 6 ≡ 5, ind 7 ≡ 11, ind 8 ≡ 3, ind 9 ≡ 8, ind 10 ≡ 10,
ind 11 ≡ 7, ind 12 ≡ 6 (mod 12).

Si le nombre p est quelque peu grand, il devient incommode de chercher quel est l'indice d'un nombre donné. On construit alors deux Tables, l'une pour les indices, l'autre pour les nombres.

Ainsi $p = 61$, $r = 10$ donnent les Tables suivantes, dans lesquelles chaque nombre N est mis sous la forme $10a + b$. Les dizaines a sont inscrites dans la première colonne verticale, les unités dans la première ligne horizontale.

Table d'indices (mod 60).

	0.	1.	2.	3.	4.	5.	6.	7.	8.	9.
0............		0	47	42	34	14	29	23	21	24
1............	1	45	16	20	10	56	8	49	11	22
2............	48	5	32	39	3	28	7	6	57	25
3............	43	13	55	27	36	37	58	33	9	2
4............	35	18	52	41	19	38	26	40	50	46
5............	15	31	54	51	53	59	44	4	12	17
6............	30									

Table des nombres (mod 61).

	0.	1.	2.	3.	4.	5.	6.	7.	8.	9.
0............	1	10	39	24	57	21	27	26	16	38
1............	14	18	58	31	5	50	12	59	41	44
2............	13	8	19	7	9	29	46	33	25	6
3............	60	51	22	37	4	40	34	35	45	23
4............	47	43	3	30	56	11	49	2	20	17
5............	48	53	42	54	52	32	15	28	36	55

Ainsi, on trouvera pour la première Table :

$$\text{ind } 1 \equiv 0, \quad \text{ind } 2 \equiv 47, \quad \ldots, \quad \text{ind } 10 \equiv 1, \quad \text{ind } 15 \equiv 56, \quad \ldots,$$
$$\text{ind}(-1) \equiv \text{ind } 60 \equiv 30 \pmod{60}.$$

La deuxième Table donne :

$$0 \equiv \text{ind } 1, \quad 1 \equiv \text{ind } 10, \quad \ldots, \quad 10 \equiv \text{ind } 14, \quad 15 \equiv \text{ind } 50, \quad \ldots.$$

12. Une Table d'indices du nombre premier p permet de résoudre facilement une congruence du premier degré (mod p).

Ainsi, soit donnée la congruence

$$13x \equiv 18 \pmod{61}.$$

Elle donne

$$x \equiv \frac{18}{13} \pmod{61} \quad \text{(II, 11)}.$$

Or,

$$\operatorname{ind} x \equiv \operatorname{ind} 18 - \operatorname{ind} 13 \equiv 11 - 20 \equiv -9 \equiv 51 \pmod{60},$$

d'où

$$x \equiv 53 \pmod{61}.$$

13. Une Table d'indices peut aussi servir pour la résolution de la congruence $x^2 \equiv a \pmod{p}$ qui fait l'objet des paragraphes (IV, 25).

Soit donnée la congruence $x^2 \equiv 57 \pmod{61}$, elle est possible, car

$$\left(\frac{57}{61}\right) = \left(\frac{-4}{61}\right) = \left(\frac{+4}{61}\right) \equiv +1.$$

Elle donne

$$2 \operatorname{ind} x \equiv \operatorname{ind} 57 \equiv 4 \pmod{60},$$

d'où

$$\operatorname{ind} x \equiv 2 \pmod{30} \quad \text{ou} \quad \operatorname{ind} x \equiv 2 \quad \text{ou} \quad 32 \pmod{60}$$

et

$$x \equiv 39 \quad \text{ou} \quad 22 \pmod{61}.$$

14. On voit, par ces exemples, l'utilité d'une Table d'indices. Il est toutefois à remarquer qu'une Table spéciale est nécessaire pour chaque nombre premier. Et même si l'on veut se contenter d'une seule Table pour chaque nombre, il ne serait pas possible d'établir une Table complète pour tous les nombres inférieurs à une certaine limite (10000 par exemple).

Jacobi a donné (Berlin, 1839) une Table d'indices pour tous les nombres inférieurs à 1000. Nous avons entrepris le travail d'une Table d'indices pour tous les nombres inférieurs à 10000 [1]. Mais tandis que Jacobi donne pour chaque nombre les deux Tables (l'une pour les indices, l'autre pour les nombres), nous nous bornons à donner pour tout nombre premier inférieur à 10000 les indices de tous les nombres premiers inférieurs à 100.

Un exemple fera comprendre le procédé que nous avons suivi pour établir les indices de tous les nombres premiers inférieurs à 100 sans calculer toutes les $(p-1)$ puissances de la racine primitive. Remarquons que nous avons depuis longtemps (1911) établi une Table donnant une racine primitive pour tout nombre inférieur à 10000. Cette Table se trouve dans le numéro spécial de mai 1911 du *Sphinx Œdipe* (Nancy, 1911).

[1] On peut se procurer chez l'auteur une copie photographique de cette Table.

15. *Problème.* — Trouver les indices de tous les nombres premiers inférieurs à 100 (mod 9649).

On prend pour base une racine primitive quelconque, par exemple $r = 7$, et l'on calcule quelques dizaines de puissances de r (mod 9649). On trouve :

	0.	1.	2.	3.	4.	5.	6.	7.	8.	9.
0........	1	7	49	343	2401	7158	1861	3378	4348	1489
1........	774	5418	8979	4959	5766	1766	2713	9342	7500	4255
2........	838	5866	2466	7313	5046	6375	6029	3607	5951	3061
3........	2129	5254	7831	6572	7408	3611	5979	3257	3501	5209
4........	7516	4367	1622	1705	2286	5353	....			

On notera les relations (mod 9649)

$$9600 \equiv -49,$$
$$7^4 . 4 \equiv -45,$$
$$7^{18} \equiv 7500,$$

ou, avec les notations,

$$\text{ind } 2 \equiv x, \qquad \text{ind } 3 \equiv y, \qquad \text{ind } 5 \equiv z,$$

on a

$$7x + y + 2z = 4826,$$
$$2x - 2y - z = 4820,$$
$$2x + y + 4z = 18,$$

ou, en éliminant z,

$$11x - 3y = 4818,$$
$$10x - 7y = 2;$$

d'où

$$47y \equiv 48\,158 \,(\text{mod } 9548) \equiv 9566 \equiv 270\,062,$$
$$y = 5746 = \text{ind } 3,$$
$$x = 1128 = \text{ind } 2,$$
$$z = 5240 = \text{ind } 5;$$

$p = 7$ étant pris pour base, on aura

$$\text{ind } 7 = 1.$$

La relation $7^{10} \equiv 774 \equiv 18.43$ donne

$$\text{ind } 43 \equiv 10 - 1128 - 2 \times 5746 \equiv 6686.$$

La relation $7^{12} \equiv 8979 \equiv -870$ donne

$$\text{ind } 29 = 12 + 4824 - (1128 + 5746 + 5240) = 2370.$$

La relation $7^{25} \equiv 6375 = 17 \times 3.215$ donne

$$\text{ind } 17 = 25 - (5746 + 305240) = 7503.$$

La relation $29 \times 336 = 9774 \equiv 95$ donne

$$\text{ind } 19 = (2370 - 4 \times 1128 + 5746 + 1) - 5240 = 7389.$$

La relation $23 \times 425 = 9775 \equiv 126$ donne

$$\text{ind } 23 = (1128 + 2.5746 + 1) - (7503 + 2.5240) \equiv 4286.$$

La relation $7^{19} \equiv 4255 \equiv 5.23.37$ donne

$$\text{ind } 37 = 19 - (5240 + 4286) \equiv 141.$$

La relation $31 \times 315 = 9765 \equiv 116$ donne

$$\text{ind } 31 = (2 \times 1128 + 2370) - (2.5746 + 5240 + 1) = 7189.$$

La relation $7^{43} \equiv 1705 \equiv 11.155$ donne

$$\text{ind } 11 = 43 - (5240 + 7189) \equiv 6910.$$

La relation $13 \times 729 = 9477 \equiv -172$ donne

$$\text{ind } 13 = (6686 + 2.1128 + 4824) - 6.5746 \equiv 8234.$$

La relation $41 \times 234 = 9594 \equiv -55$ donne

$$\text{ind } 41 \equiv (5240 + 6910 + 4824) - (1128 + 2.5746 + 8234) \equiv 5768.$$

La relation $47 \times 205 \equiv 9635 \equiv -14$ donne

$$\text{ind } 47 \equiv (1128 + 1 + 4824) - (5240 + 5768) \equiv 4590.$$

La relation $53 \times 182 = 9646 \equiv -3$ donne

$$\text{ind } 53 \equiv (5746 + 4824) - (1128 + 1 + 8234) \equiv 1207.$$

La relation $59 \times 164 = 9676 \equiv 27$ donne

$$\text{ind } 59 \equiv 3.5746 - (2.1128 + 5768) \equiv 9214.$$

La relation $61 \times 159 = 9699 \equiv 50$ donne

$$\text{ind } 61 \equiv (2.5240 + 1128) - (2.5746 + 1207) \equiv 8557.$$

La relation $67 \times 143 \equiv 9581 \equiv -68$ donne

$$\text{ind } 67 \equiv (2.1128 + 7503 + 4824) - (6910 + 8234) \equiv 9087.$$

La relation $71 \times 136 \equiv 9656 \equiv 7$ donne

$$\text{ind } 71 \equiv 1 - (3.1128 + 7503) \equiv 8410.$$

La relation $73 \times 133 \equiv 9709 \equiv 60$ donne

$$\text{ind } 73 \equiv (2 + 1128 + 5746 + 5240) - (1 + 4286) \equiv 8955.$$

La relation $79 \times 121 \equiv 9559 \equiv -90$ donne

$$\text{ind } 79 \equiv (1128 + 2.5746 + 5240 + 4824) - 2.6910 \equiv 8864.$$

La relation $83 \times 117 \equiv 9771 \equiv 62$ donne

$$\text{ind } 83 \equiv (1128 + 7189) - (2.5746 + 8234) \equiv 7987.$$

La relation $89 \times 108 \equiv 9612 \equiv -37$ donne

$$\text{ind } 89 \equiv (141 + 4824) - (2.1128 + 3.5746) \equiv 4767.$$

La relation $9700 \equiv 51$ donne

$$\text{ind } 97 \equiv (5746 + 7503) - 2(1128 + 5240) \equiv 513.$$

16. Cette Table abrégée est naturellement moins commode que la double Table complète que nous avons établie précédemment. Toutefois, elle rend suffisamment de services pour justifier le travail demandé pour son établissement.

D'abord, connaissant les indices de tous les nombres premiers inférieurs à 100, on trouve facilement l'indice de n'importe quel nombre. Par exemple, pour trouver l'indice de N, on opérera de la façon suivante :

1° Si N est composé de facteurs premiers inférieurs à 100, on aura l'indice de N par la somme des indices de ses facteurs.

Ainsi, pour $p = 9649$,

$$\text{ind } 143 = \text{ind } 11 + \text{ind } 13 = 6910 + 8234 = 15144 \equiv 5496 \pmod{9648}.$$

2° Si N est premier, on prendra une relation quelconque de la forme $a\mathrm{N} \equiv b \pmod{p}$ avec a et b inférieurs à 100 ou composés de facteurs inférieurs à 100, ce qui est toujours possible.

Par exemple, pour trouver l'indice de 1021 (mod 9649), on prendra la relation

$$10.1021 \equiv 561 \equiv 3.11.17$$

donnant

$$\begin{aligned} \text{ind } 1021 &\equiv (\text{ind } 3 + \text{ind } 11 + \text{ind } 17) - (\text{ind } 2 + \text{ind } 5) \\ &= (5746 + 6910 + 7503) + (1128 + 5240) = 13791 \equiv 4143 \\ &\pmod{9648}. \end{aligned}$$

Ensuite il est facile de trouver un nombre $\mathrm{N} \pmod{p}$ dont on connaît l'indice $i \pmod{p-1}$. En effet, r étant la racine primitive qui a servi pour le calcul des indices, on aura

$$\mathrm{N} \equiv r^i \pmod{p}.$$

Par exemple, si l'on connaît, pour le module 9649,

$$\text{ind N} \equiv 6368 \pmod{9648},$$

on aura

$$\mathrm{N} \equiv 7^{6368} \pmod{9649}.$$

Or,

$$\mathrm{N} \equiv 7^{6368} \equiv -7^{6368-4824} \equiv -7^{1544} \pmod{9649}.$$

Puisqu'on trouve parmi les indices connus ind 97 ≡ 513, on a

$$7^{513} \equiv 97, \qquad \text{d'où} \qquad 2^{1539} \equiv 97^3$$

et

$$\begin{aligned} \mathrm{N} &\equiv -97^3.7^5 \equiv -97.9409.7158 \equiv +97.240.7158 \\ &\equiv 240.9247 \equiv -240.402 \equiv -96480 \equiv +10. \end{aligned}$$

17. Théorème. — *La congruence $x^m \equiv \mathrm{A} \pmod{p}$ n'est possible que si l'indice de* A *est un multiple de m, m étant supposé un des diviseurs de $p-1$.*

En effet, cette congruence donne

$$m \text{ ind } x = \text{ind A} \pmod{p-1}.$$

Or, si $p-1$ est divisible par m, il faut que ind A le soit aussi. On aura alors

$$\operatorname{ind} x = \frac{\operatorname{ind} A}{m} \left(\operatorname{mod} \frac{p-1}{m}\right),$$

ce qui donnera m solutions pour ind x (mod $p-1$) et, partant, m solutions pour x (mod p).

18. Si l'on ne possède pas de Table d'indices, on peut encore être fixé sur la possibilité ou l'impossibilité de la congruence $x^m \equiv A \pmod p$ de la manière suivante :

Soit q le quotient de $p-1$ par m, de sorte que $p-1=mq$. Si l'on élève les deux membres de la congruence $x^m \equiv A \pmod p$ à la puissance q, il vient

$$x^{mq} \equiv A^q \quad \text{ou} \quad x^{p-1} \equiv A^q \pmod p;$$

or,

$$x^{p-1} \equiv 1 \pmod p;$$

donc on aura

$$A^q \equiv 1 \pmod p.$$

Ainsi, si la congruence $x^m \equiv A \pmod p$ est possible, on aura

$$A^{\frac{p-1}{m}} \equiv 1 \pmod p,$$

Inversement, si l'on a

$$A^{\frac{p-1}{m}} \equiv 1 \pmod p,$$

la congruence $x^m \equiv A \pmod p$ est possible. En effet, soient r une racine primitive de p et i l'indice de A dans ce système; donc

$$r^i \equiv A \pmod p.$$

Puisque

$$r^{iq} = A^q \equiv A^{\frac{p-1}{m}} \equiv 1 \pmod p,$$

on aura

$$iq \equiv p-1 \pmod{p-1} \quad \text{ou} \quad iq \equiv 0 \pmod{p-1}$$

ou

$$i \equiv 0 \left(\operatorname{mod} \frac{p-1}{q} = m\right).$$

Ainsi i est un multiple de m, ce qui établit la possibilité de la

congruence

$$x^m \equiv A \pmod{p}.$$

19. Comme nous l'avons dit, il y a plusieurs systèmes d'indices. A chaque racine primitive correspond un système d'indices. Il est du reste facile de passer d'un système d'indices à un autre.

Soit r la base d'un système d'indices et supposons qu'on veuille trouver l'indice d'un nombre N dans une autre base r'.

On aura donc, x désignant l'indice de N dans la base r' et i l'indice de N dans la base r,

$$A \equiv r^i \equiv r'^x \pmod{p}$$

ou

$$i \operatorname{ind} r \equiv x \operatorname{ind} r' \pmod{p-1};$$

or

$$\operatorname{ind} r \equiv 1,$$

d'où

$$x \equiv \frac{i}{\operatorname{ind} r'} \pmod{p-1},$$

ce symbole devant être interprété comme nous l'avons dit (II, 11). Mais quelle que soit la base choisie, on aura toujours :

$$\operatorname{ind} 1 \equiv 0 \pmod{p-1},$$

$$\operatorname{ind}(-1) \equiv \operatorname{ind}(p-1) \equiv \frac{p-1}{2} \pmod{p-1},$$

relations que nous avons établies (V, 9) et qui sont indépendantes de la base choisie.

20. En supposant toujours que le module p est un nombre premier supérieur à 2, étudions maintenant la congruence

$$a^x \equiv 1 \pmod{p}.$$

On voit facilement que si $x \equiv r$ est une solution, $x \equiv kr$ en est une aussi, la solution générale étant

$$x = kr + n(p-1) \quad \text{ou} \quad x \equiv kr \pmod{p-1}.$$

Si ensuite d est le plus grand commun diviseur de r et $p-1$, $x = d$ satisfait encore à la congruence $a^x \equiv 1 \pmod{p-1}$. Il en résulte que la plus petite solution de cette congruence est d, d étant

un diviseur de $p-1$, en comprenant parmi les diviseurs de $p-1$ le nombre $p-1$ aussi.

Ainsi, si d est la plus petite solution de cette congruence, toutes les solutions sont

$$x \equiv kd \pmod{p-1} \quad \text{ou simplement} \quad x \equiv 0 \pmod{d}.$$

Ainsi, la plus petite solution de la congruence

$$2^x \equiv 1 \pmod{229153}$$

est $x \equiv 176$ et toutes les solutions sont $x \equiv 0 \pmod{176}$.

Il en résulte que

$$2^{176} \equiv 1 \pmod{229153},$$

d'où

$$2^{88} \equiv -1 \pmod{229153};$$

donc $2^{88}+1$ est divisible par 229153.

[On ne peut pas avoir $2^{88} \equiv +1 \pmod{229153}$, car la plus petite solution serait alors $x = 88$ et non $x = 176$.]

Nous avons établi une Table donnant la plus petite solution de la congruence $2^x \equiv 1 \pmod{p}$ pour tous les nombres premiers p inférieurs à 300000 [1].

21. Théorème. — *Si la plus petite solution de la congruence* $a^x \equiv 1 \pmod{p}$ *est* m, *l'indice de* a *est divisible par*

$$\frac{p-1}{m} = q.$$

En effet, on aura

$$x \operatorname{ind} a \equiv 0 \pmod{p-1},$$

donc

$$m \operatorname{ind} a \equiv 0 \pmod{p-1},$$

ce qui exige que $\operatorname{ind} a$ soit divisible par $\frac{p-1}{m}$ ou par $q = \frac{p-1}{m}$.

On dit que a est un résidu de $q^{\text{ième}}$ de p et l'on écrit $\left(\frac{a}{p}\right)_q = 1$. On trouvera à la fin une Table (IV) de résidus $q^{\text{ièmes}}$ de p avec

$$q = 2.3.4.5.6.7.8.9.10.14.16.18.$$

Ainsi, quelle que soit la base qui a servi pour l'établissement du

---

(1) On peut se procurer chez l'auteur une copie photographique de cette Table.

système d'indices, on aura toujours

$$D(\text{ind } a, p-1) = q,$$

$D(x, y)$ désignant le plus grand commun diviseur de x et y, car cette relation montre que la plus petite solution de la congruence $a^x \equiv 1 \pmod{p}$ est

$$m = \frac{p-1}{q}$$

et cette plus petite solution est évidemment indépendante du choix de la base

Cette relation est un invariant d'un système d'indices.

22. Inversement, si le plus grand commun diviseur de ind a et $p-1$ est q, la plus petite solution de la congruence $a^x \equiv 1 \pmod{p}$ est

$$x \equiv \frac{p-1}{q}.$$

Soient r la base choisie et i l'indice de a, donc

$$r^i \equiv a \pmod{p}.$$

Puisque i est divisible par q, on aura

$$i = qq'$$

ou

$$r^{qq'} \equiv a \pmod{p}$$

ou, en désignant $r^{q'}$ par r', il vient

$$r'^q \equiv a \pmod{p}.$$

Si l'on élève les deux membres à la puissance $\frac{p-1}{q}$, on aura

$$r'^{p-1} \equiv a^{\frac{p-1}{q}} \equiv 1 \pmod{p}.$$

Ainsi $a^x \equiv 1 \pmod{p}$ est vérifié pour $x = \frac{p-1}{q}$.

Il est facile de démontrer que c'est la plus petite solution.

23. Il résulte de ce qui précède que, relativement au module p, les nombres non divisibles par p se répartissent de la façon suivante :

Soient $d_1 = 1$, $d_2 = 2$, d_3, d_4, ..., $d_n = p - 1$ les n diviseurs du nombre $p - 1$.

Il y aura :

$\varphi(p-1)$ nombres tels que la plus petite solution de $a^x \equiv 1 \pmod{p}$ est $x = p-1$,
$\varphi(d_{n-1})$ » $x = d_{n-1}$,
....,
$\varphi(d_i)$ » $x = d_i$,
$\varphi(2) = 1$ » $x = 2$,
$\varphi(1) = 1$ » $x = 1$.

(On aura $x = 2$ si $a = p - 1$, et $x = 1$ si $a = 1$.)

De cette façon, tous les $p - 1$ nombres sont classés, car

$$\varphi(p) = p - 1 = \varphi(p-1) + \varphi(d_{n-1}) + \ldots + \varphi(d_i) + \ldots + \varphi(2) + \varphi(1) \quad (\text{I}, 19).$$

Exemple. — $p = 61$, $\varphi = 60$, $n = 12$ (nombre de diviseurs de 60) :

n.	d_n.	$\varphi(d_n)$.	N.
1	1	1.........	1
2	2	1.........	60
3	3	2.........	13.47
4	4	2.........	11.50
5	5	4.........	3.20.34.58
6	6	2.........	14.48
7	10	4.........	9.27.41.52
8	12	4.........	21.29.32.40
9	15	8.........	12.15.16.22.25.42.56.57
10	20	8.........	8.23.24.28.33.37.38.53
11	30	8.........	4.5.19.36.39.45.46.49
12	60	16.........	2.6.7.10.17.18.26.30.31.35.43.44.51.54.55.59

Les nombres de la colonne N sont ceux qui satisfont à la congruence $\chi^{d_i} \equiv 1 \pmod{61}$, sans satisfaire à une congruence de la même forme, mais avec un plus petit exposant. En d'autres termes, les nombres de la colonne N sont les racines primitives des congruences $\chi^{d_i} \equiv 1 \pmod{61}$. Tous les $\varphi(61) = 60$ nombres inférieurs à 61 et premiers avec 61 figurent dans cette colonne.

24. Théorème. — *Les diviseurs primitifs d'un nombre de la*

forme $a^m - 1$ *sont de la forme* $km+1$, *les diviseurs primitifs d'un nombre de la forme* a^m+1 *sont de la forme* $2km+1$, *les diviseurs primitifs d'un nombre de la forme* $2^{4m}+1$ *sont de la forme* $16mk+1$.

Nous avons vu (III, 5) ce qu'on entend par diviseur primitif. Soit p un diviseur primitif de $a^m - 1$, on aura

$$a^m \equiv 1 \pmod{p}.$$

Puisque p est un diviseur primitif, la congruence

$$a^x \equiv 1 \pmod{p}$$

admet, comme plus petite solution, la solution $x = m$, diviseur de $p-1$. Ainsi $p-1$ est divisible par m.

Si l'on pose $p - 1 = mk$, on aura

$$p = mk + 1.$$

Si l'on a

$$a^m + 1 \equiv 0 \pmod{p},$$

on a aussi

$$a^{2m} \equiv 1 \pmod{p},$$

donc

$$p = 2mk + 1.$$

Soit enfin

$$2^{4m} + 1 \equiv 0 \pmod{p}.$$

On aura

$$2^{8m} \equiv 1 \pmod{p},$$

ce qui donne

$$p = 8mq + 1.$$

Nous allons démontrer que q est pair.

En effet, on a

$$\left(\frac{2}{p}\right) = \left(\frac{2}{8mq+1}\right) = +1,$$

donc 2 est résidu quadratique de p; donc

$$2^{\frac{p-1}{2}} \equiv 2^{4mq} \equiv 1 \pmod{p}.$$

Il en résulte que $4mq$ est divisible par $8m$, ce qui exige que q soit pair.

Posons $q = 2k$, on aura

$$p = 8mq + 1 = 16mk + 1.$$

Ainsi les diviseurs de $2^{32} + 1$ doivent être de la forme $4.32k + 1$ ou $128k + 1$. Le premier nombre premier de cette forme est 641 qui effectivement divise $2^{32} + 1$ (I, 4; II, 6).

25. Supposons maintenant que le module p n'est pas premier. Si le module p contient plusieurs facteurs premiers a^m, b^n, ..., on décomposera la congruence donnée en plusieurs, dont les modules sont a^m, b^n, ...

Supposons donc que le module est une puissance d'un nombre premier impair, $p = a^m$.

Si r est une racine primitive du nombre a, r est aussi une racine primitive du nombre $p = a^m$ et l'on aura

$$r^{(a-1)a^{m-1}} \equiv 1 \quad (\text{mod } p) \quad (\text{III}, 3).$$

Si l'on construit une Table d'indices avec la base r, la Table contiendra les indices de tous les $\varphi(p) = (a - 1)a^{m-1}$ nombres inférieurs à $p = a^m$ et premiers avec p, donc non divisibles par a.

Ainsi tout nombre non divisible par p a un indice et inversement.

Toutes les relations que nous avons établies restent vraies, sauf à remplacer pour les indices le module $p - 1$ par le module

$$\varphi(p) = (a - 1)a^{m-1}.$$

26. Si, enfin, le module est une puissance de 2, on peut prendre pour base soit le nombre 3, soit le nombre 5.

Si l'on prend pour base le nombre 3, seuls les nombres de la forme $8k + 1.3$ auront un indice. De même, si l'on prend pour module le nombre 5, seuls les nombres $8k + 1.5$ auront un indice.

Il est donc nécessaire de modifier la définition des indices pour le cas du module 2^n.

On adoptera, par exemple, la définition suivante :

$$3^i \equiv (-1)^{\frac{(N-1)(N-3)}{8}} . N \quad (\text{mod } 2^n).$$

Ainsi avec le module $2^5 = 32$, on obtient :

$$\begin{array}{rcccccccccl} i = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & & (\text{mod } 8), \\ \pm 3^i = & 3 & 9 & 5 & 15 & 13 & 7 & 11 & 1 & & (\text{mod } 32). \end{array}$$

Ainsi les indices de

$$1 \quad 3 \quad 5 \quad 7 \quad 9 \quad 11 \quad 13 \quad 15 \qquad (\text{mod } 32)$$

seront

$$0 \quad 1 \quad 3 \quad 6 \quad 2 \quad 7 \quad 5 \quad 4 \qquad (\text{mod } 8).$$

Nous nous réservons de développer ultérieurement ce sujet plus en détail.

CHAPITRE VI.

FACTORISATION.

1. Une des applications de la théorie qui précède est la factorisation des grands nombres. Par un court historique de la question, on verra le progrès de ce problème pendant les 50 dernières années.

En 1772, Euler a démontré que le nombre

$$2\,147\,483\,647 = 2^{31} - 1$$

est premier, et c'était le plus grand nombre premier connu à cette époque.

En 1875, Lucas écrit (*Nouvelles Annales de Mathématiques*, 1875, p. 523) qu'il n'a pu vérifier si le nombre

$$8\,831\,418\,697 = \frac{2^{41}+1}{3.83}$$

est premier. Il ajoute : « Il serait facile de s'assurer si ce nombre est premier, et, dans le cas de réussite, ce serait, je pense, le plus grand nombre premier connu actuellement. »

Lucas semble ignorer, en 1875, les travaux de Landry (Paris, 1867 et 1869), où sont donnés plusieurs nombres premiers bien plus grands que celui cité par Lucas.

Et cependant trois ans plus tard Lucas a surpassé Landry. En 1878, Lucas a donné la factorisation de $2^n \pm 1$ pour des valeurs de n dépassant de beaucoup celles de Landry.

Nous n'avons relevé dans les travaux de Lucas que les erreurs suivantes; de ces résultats, la décomposition de $2^{64}+1$ a été donnée par Landry en 1880 à l'âge de 82 ans et celle de $2^{77}+1$ par Cunningham en 1910 :

$2^{99} - 1 = (7 \times 23 \times 73 \times 89 \times 599479) \times (199 \times 153649 \times 33057806959),$

$2^{77} + 1 = (3 \times 43 \times 683) \times (617 \times 78233 \times 35532364099),$

$2^{91} + 1 = (3 \times 43 \times 2731) \times (224771 \times 31266402706564481),$

$2^{80} + 1 = 65537 \times (414721 \times 44479210368001),$

$2^{64} + 1 = 274177 \times 67280421310721,$

$2^{76} + 1 = 17 \times (1217 \times 148961 \times 24517014940753),$

$2^{82} + 1 = 5 \times (10169 \times 43249589) \times (181549 \times 12112549),$

$2^{106} + 1 = 5 \times 1800439824104653 \times (15358129 \times 586477649),$

$2^{122} + 1 = 5.733.1709.368140581013.(3456749.667055378149),$

$2^{198} + 1 = (5.109.397.4327489) \times (42373.15975607282273)$
$\times (13.37.2113.312709) \times (235621.8463901912489).$

Depuis cette époque, on a étudié des nombres laissant loin derrière eux ceux qui ont été envisagés par Euler ou par Lucas en 1875.

Ainsi l'on sait actuellement que les nombres $2^{61} - 1$, $2^{89} - 1$, $2^{107} - 1$, $2^{127} - 1$, $5.2^{75} + 1$ sont premiers et, par contre, que les nombres $2^{128} + 1$, $2^{256} + 1$ sont composés, mais on ne connaît pas les facteurs de ces nombres.

2. Si le problème de la factorisation n'a pas fait de progrès sensibles jusqu'en ces tout derniers temps, c'est à cause des difficultés spéciales qu'il présente.

Il est, en effet, facile de vérifier si un nombre donné, quelque grand qu'il soit, divise un autre nombre donné, puisque la vérification se fait par division, c'est-à-dire par un procédé direct; mais le problème inverse, c'est-à-dire le produit de deux nombres étant donné, en trouver les facteurs, résulte essentiellement du tâtonnement; et le perfectionnement des procédés n'est qu'un perfectionnement des tâtonnements, en ce sens qu'on ne fait pas d'essais pour certains cas qu'on élimine d'avance comme ne pouvant satisfaire à certaines conditions.

Remarquons d'abord que la factorisation peut se faire par deux procédés :

1° Par la recherche directe des facteurs;

2° En ramenant le nombre donné à une forme connue, dont la plus simple est une différence entre deux carrés.

C'était surtout le premier procédé qui était en usage depuis l'antiquité, et Fibonacci (1202) donne pour la première fois la règle connue d'essayer tous les facteurs possibles inférieurs à la racine carrée du nombre donné.

Fermat et Euler ont perfectionné ce procédé en se servant de formes linéaires des diviseurs. Ainsi, si par exemple le nombre donné peut être mis sous la forme $a^2 + b^2$, les diviseurs ne peuvent être que de la forme $4k + 1$. Il en résulte qu'il est inutile d'essayer la division par les nombres premiers de la forme $4k + 3$.

La connaissance de chaque forme quadratique réduit environ deux fois le nombre d'essais à faire. Il en résulte que si l'on connaît une dizaine de formes quadratiques, on réduira environ 2^{10} fois le nombre d'essais à faire, ou d'environ 1000 fois.

Quand il s'agit de décomposer un nombre de 8-10 chiffres, le procédé peut encore être employé avec succès. C'est pourquoi nous allons donner quelques détails sur son application.

On trouvera à la fin de ce Volume des Tables donnant les diviseurs linéaires de formes quadratiques $x^2 \pm Dy^2$ pour toutes les valeurs de D inférieures à 200.

On a omis les valeurs de D qui sont divisibles par un carré, car si l'on a $D = aK^2$ la forme

$$x^2 + Dy^2 = x^2 + a(Ky)^2$$

ne diffère guère de la forme plus simple $x^2 + ay^2$.

L'emploi de ce procédé est très simple. Après avoir trouvé plusieurs représentations quadratiques, telles que $x^2 \pm Dy^2$, on construit, en premier lieu, une Table des nombres premiers convenant pour les formes les plus simples, et l'on exclut de cette Table les nombres qui ne satisfont pas aux formes linéaires correspondant aux formes quadratiques restantes.

Ainsi, ayant trouvé la représentation

$$x^2 + y^2,\quad x^2 + 2y^2,\quad x^2 - 3y^2,\quad x^2 - 7y^2,\quad x^2 + 10y^2,\quad x^2 + 13y^2,$$
$$x^2 - 21y^2,\quad x^2 - 31y^2,\quad x^2 + 86y^2,$$

on procède de la façon suivante :

1° Les diviseurs linéaires de $x^2 + y^2$ sont $4K + 1$ et ceux de la

forme $x^2 + 2y^2$ sont $8K + 1.3$; donc $8K + 1$ est la seule forme linéaire qui convient aux deux formes quadratiques.

2° Les diviseurs linéaires de la forme $x^2 - 3y^2$ étant $12K \pm 1$ ou $24K + 1.11.13.23$, seule la forme $24K + 1$ coïncide avec la forme trouvée précédemment.

3° Les diviseurs linéaires de la forme $x^2 - 7y^2$ sont $28K \pm 1.3.9$ ou

$$168K \pm 1.3.9.19.25.27.29.31.37.47.53.55.57.59.65.75.81.83,$$

dont les formes $168K + 1.25.121$ seules satisfont à toutes les formes considérées jusqu'ici.

4° Ces formes développées suivant le module $840 (= 5 \times 168)$ donnent les formes

$$840K + 1.25.121.169.193.289.337.351.457.505.529.625.673.697.793$$

dont les formes

$$840K + 1.121.169.289.361.529$$

seules sont diviseurs de la forme $x^2 + 10y^2$ et des formes précédemment envisagées.

Il reste à utiliser les formes $x^2 + 13y^2$, $x^2 - 21y^2$, $x^2 - 31y^2$, $x^2 + 86y^2$.

De ces formes, $x^2 - 21y^2$ n'apprend rien de nouveau, car elle résulte des formes $x^2 - 3y^2$, et $x^2 - 7y^2$ déjà envisagées. En effet, si 3 et 7 sont résidus d'un nombre quelconque, $3 \times 7 = 21$ le sera aussi, la forme $x^2 + 86y^2$ peut être remplacée par $x^2 - 43y^2$, car si -86 et -2 sont résidus $(-86) : (-2) = +43$ l'est aussi (-2 est résidu à cause de la forme $x^2 + 2y^2$).

Il reste ainsi à utiliser les formes $x^2 + 13y^2$, $x^2 - 31y^2$ et $x^2 - 43y^2$.

Avant de le faire, formons une Table des nombres premiers inférieurs à la racine carrée du nombre considéré et des formes

$$840K + 1.121.169.289.361.529.$$

Si, par exemple, la limite est 12000 (ce qui correspond à un

nombre voisin de 144000000), on aura :

		Pour la forme.
D =	2521.3361.4201.5881.7561.9241..........	840K + 1
	1801.6841.7681.8521.................. ..	121
	1009.2689.3529.5209.....................	169
	1129.8689.10369.........................	289
	1201.4561.8761.9601.....................	361
	3049.3889.4729.5569.8089.8929.9769......	529

De ces nombres, seuls les suivants sont diviseurs de la forme x^2+13y^2 :

$$D = 2521.5209.6841.8089.8761,$$

dont $D = 2521.5209.8761$ sont diviseurs de la forme x^2-31y^2 et dont $D = 5209$ seul est diviseur de la forme x^2-43y^2.

Ainsi il suffira d'essayer la division du nombre donné par 5209 pour le factoriser ou être fixé sur sa primalité.

Donc toute la question se résume à trouver des formes quadratiques du nombre donné. On peut y arriver par les deux procédés que nous allons indiquer.

On sait que le développement de $\sqrt{N}$ en fractions continues donne lieu à une fraction continue périodique. Si un quotient complet quelconque est

$$X_n = \frac{B_n+\sqrt{N}}{D_n} = a_{n+1} + \frac{1}{X_{n+1}},$$

$(-1)^n D^n$ est résidu de N et N ou son multiple peut être représenté par la forme $x^2+(-1)^n Dy^2$.

De là résulte une règle très simple pour trouver autant de représentations quadratiques qu'on voudra. Toutefois, si le nombre des termes de la période est petit, ces formes peuvent ne pas suffire. Cela arrive, en particulier, pour $N = a^2+1$ et dans bien d'autres cas.

On considérera alors le développement de $\sqrt{2A}$, ou celui de $\sqrt{3A}$ ou, d'une façon générale de $\sqrt{nA}$, étant donné que tout résidu de nA est aussi résidu de A.

Toutefois, le développement de $\sqrt{A}$ est assez laborieux et une méthode de tâtonnements est, dans bien des cas, préférable.

Soit N un nombre impair sur la nature duquel on n'est pas fixé. Soit encore a le plus grand entier dont le carré est inférieur à N.

Posons

$$N = (a + x)^2 + r,$$

x étant choisi de façon à rendre r divisible par des carrés. D'une façon générale, on trouve plusieurs valeurs de x pour lesquelles r devient un carré, le double d'un carré, le triple d'un carré, etc.

Voici comment on procédera : On déterminera uue série de congruences linéaires :

$$N \equiv r_2 \pmod{2^3} \equiv r_3 \pmod 3 \equiv r_5 \pmod 5 \equiv \ldots \equiv r_p \pmod p.$$

Si $N \equiv r_p \pmod p$ est un résidu quadratique, on déterminera $N \equiv r'_p \pmod{p^2}$. La solution de la congruence auxiliaire

$$z^2 \equiv r'_p \qquad \pmod p$$

nous fournira deux valeurs de z telles qu'en posant

$$a \pm x = z$$

on aura

$$r \equiv 0 \pmod{p^2} \text{ ou } r = Kp^2 \qquad \text{et} \qquad N = (a + x)^2 + Kp^2.$$

Un exemple fera comprendre la marche à suivre :

Soit donné le nombre 123456789 exprimé en système décimal par les neuf chiffres significatifs. On a

$$123456789 = 9 . 13717421.$$

Posons

$$N = 13717421$$

et proposons-nous de décomposer ce dernier nombre.

On a

$$\begin{aligned} N &\equiv 5 \pmod 8 \equiv 2 \pmod 3 \equiv 1 \pmod 5 \equiv 4 \pmod 7 \equiv 3 \pmod{11} \\ &\equiv 3 \pmod{13} \equiv 2 \pmod{17} \equiv 10 \pmod{19} \equiv 14 \pmod{23} \\ &\equiv 15 \pmod{29} \equiv 14 \pmod{31} \equiv 4 \pmod{37} \ldots, \end{aligned}$$

$$\begin{aligned} N &\equiv 21 \pmod{25} \equiv 18 \pmod{49} \equiv 14 \pmod{121} \equiv 29 \pmod{169} \\ &\equiv 36 \pmod{289} \equiv 107 \pmod{961} \equiv 41 \pmod{1369}; \end{aligned}$$

d'où

$$\pm z \equiv 11 \pmod{25} \equiv 19 \pmod{49} \equiv 16 \pmod{121} \equiv 69 \pmod{169}$$
$$\equiv 6 \pmod{289} \equiv 359 \pmod{961} \equiv 331 \pmod{1369}.$$

On a, de plus,

$$N = 3703^2 + 5212 = (3703 - x)^2 + r.$$

On a

$$N = 3711^2 - 541.10^2 = 3689^2 + 1087.10^2 = 3661^2 + 3145.10^2$$
$$= 3639^2 + 4751.10^2 \ldots$$

$$N = 3694^2 + 1465.7^2 = 3743^2 - 1493.14^2 = 3645^2 + 2201.14^2 \ldots$$
$$= 3735^2 - 731.22^2 = 3767^2 - 977.22^2 = 3646^2 + 701.11^2 = 3614^2 + 211.55^2 \ldots$$
$$= 3787^2 - 907.26^2 = 3649^2 + 595.52^2 = 5408^2 - 707 \times 143^2 \ldots$$
$$= 3763^2 - 383.34^2 = 3751^2 - 305.34^2 = 3474^2 + 5705.17^2 = 3462^2 + 5993.17^2 \ldots$$
$$= 4203^2 - 1027.62^2 = 3485^2 + 409.62^2 \ldots$$
$$= 3776^2 - 395.37^2 \ldots$$

On a ainsi les résidus suivants :

541 ; -1087 ; $-3145 = -5.17.37$; -4751 ; $-1465 = -5.293$;
1493 ; $-2201 = -31.71$; $731 = 17.43$; 977 ; -701 ; -211 ;
907 ; $-595 = -5.7.17$; $707 = 7.101$; 383 ; $305 = 5.61$;
$-5705 = -5.7.163$; $-5993 = -13.461$; $1027 = 13.79$;
-409 ; $395 = 5.79$.

Si l'on y ajoute les formes

$$N = 761^2 + 7 \times 1370^2 = 3429^2 + 5.626^2,$$

on aura les résidus -7, -5 qui, combinés avec les résidus trouvés précédemment, donnent les résidus

$$-17; \quad -61; \quad -101; \quad -43; \quad -79; \quad -13$$

ou les formes

$x^2 + 13y^2$; $x^2 + 17y^2$; $x^2 + 43y^2$; $x^2 + 61y^2$; $x^2 + 79y^2$; $x^2 + 101y^2$.

Les diviseurs communs aux deux formes $x^2 + 5y^2$ et $x^2 + 7y^2$ sont

$$140K + 1.9.23.29.43.67.81.107.109.121.123.127$$

qui donnent les nombres premiers suivants comme diviseurs éventuels de N :

23.29.43.67.107.109.127.149.163.263.281.347.389.401.421.443.449.463.
487.541.547.569.641.683.701.709.743.809.821.823.827.863.883.907.947.
967.1009.1061.1087.1103.1129.1163.1201.1229.1283.1289.1303.1327.1367.
1381.1409.1423.1429.1481.1523.1549.1583.1607.1621.1663.1667.1709.1723.
1747.1787.1789.1801.1901.2003.2027.2069.2081.2083.2087.2129.2143.
2207.2221.2269.2347.2381.2389.2423.2447.2503.2521.2543.2549.2647.2683.
2689.2741.2767.2801.2843.2909.2927.2963.2969.3049.3061.3067.3089.
3109.3187.3203.3221.3229.3301.3329.3343.3347.3361.3389.3467.3469.3529.
3581.3607.3623.

De ces nombres, seuls les suivants sont diviseurs de la forme $x^2 + 13y^2$:

29.67.163.389.463.487.569.641.683.701.743.809.827.863.947.967.1087.
1103.1163.1367.1381.1423.1429.1481.1523.1607.1621.1723.1747.1787.1901.
2081.2087.2129.2143.2347.2389.2423.2503.2521.2543.2549.2647.2683.
2767.2909.2927.3187.3203.3221.3301.3329.3343.3347.3389.3706.

De ces nombres, les suivants sont diviseurs de la forme $x^2 + 17y^2$:

163.389.487.569.683.743.827.947.1163.1367.1381.1423.1429.1481.1523.
1723.2189.2389.2543.2549.2647.2683.2909.2927.3207.3221.3343.3607.

Seuls les nombres suivants sont diviseurs de la forme $x^2 + 43y^2$:

487.569.683.827.947.1381.1423.2389.2543.2647.2683.3207.3607.

Seuls les suivants sont diviseurs de la forme $x^2 + 61y^2$:

569.683.947.1381.2543.2647.3607.

Seuls les suivants sont diviseurs de la forme $x^2 + 79y^2$:

569.683.1381.2647.3607.

Seuls les nombres 569.1381.3607 sont diviseurs de la forme $x^2 + 101y^2$.

Ainsi, si N n'est pas premier, il est divisible par un de ces

nombres. On trouve, en effet,

$$N = 3607 \times 3803 \qquad \text{et} \qquad 123456789 = 9 \times 3607 \times 3803.$$

Ce procédé est inapplicable dès qu'il s'agit d'un nombre supérieur à 10^{14}, étant donné qu'on ne possède pas de Table de nombres premiers au delà de 10 millions.

C'est donc le second procédé que nous allons étudier.

3. Avant d'aborder la décomposition d'un nombre par l'équation $X^2 - Y^2 = N$, examinons quelques autres procédés de factorisation indirecte.

Si le nombre donné est de la forme $4k+1$, on peut essayer la décomposition de N en somme de deux carrés. Dès lors, si l'on ne trouve aucune solution (si l'on est certain qu'il n'en existe aucune) le nombre est composé des facteurs (en nombre pair) de la forme $4k+3$. S'il n'existe qu'une solution, le nombre est premier. Si l'on en trouve plusieurs, le nombre est composé de facteurs de la forme $4k+1$.

Dans ce dernier cas, on trouve les facteurs de la façon suivante. Supposons qu'on ait trouvé

$$N = a^2 + b^2 = c^2 + d^2.$$

Posons

$$N = (x^2+y^2)(z^2+t^2) = (xz \pm yt)^2 + (xt \pm yz)^2,$$

d'où

$$xz + yt = a, \qquad xz - yt = c,$$

et

$$xt - yz = b, \qquad xt + yz = d,$$

ou

$$xz = \frac{1}{2}(a+c), \quad yt = \frac{1}{2}(a-c), \quad xt = \frac{1}{2}(d+b), \quad yz = \frac{1}{2}(d-b).$$

(On suppose que a et c de même que b et d sont de même parité, c'est-à-dire tous les deux pairs ou tous les deux impairs, ce qui est toujours possible.)

Ce système n'aurait pu être résolu d'une façon générale, car

$$(xz)(yt) = (xt)(yz);$$

donc les quatre autres équations se réduisent à trois; mais puisque

x, y, z et t sont des entiers, on aura

$$\frac{xz}{yz} = \frac{\frac{1}{2}(a+c)}{\frac{1}{2}(d-b)} = \frac{a+c}{d-b} = \frac{m}{n},$$

m et n étant premiers entre eux ; d'où

$$x = m, \qquad y = n,$$

et l'un des facteurs est

$$x^2 + y^2 = m^2 + n^2.$$

Exemples. — 1° Le nombre 133 est de la forme $4k+1$, mais ne peut pas être mis sous la forme x^2+y^2, donc 133 contient un nombre pair de facteurs de la forme $4k+3$. On trouve, en effet, $133 = 7.19$; il en est de même de $1729 = 7.13.19$.

2° Le nombre $89 = 8^2 + 5^2$ ne peut pas être mis autrement sous la forme x^2+y^2, donc 89 est premier.

C'est de cette façon qu'Euler a trouvé que le nombre 1009 1401 est premier comme ne pouvant se mettre sous la forme de x^2+y^2 que d'une façon avec $x = 2920$, $y = 1251$.

3° Le nombre

$$221 = 14^2 + 5^2 = 10^2 + 11^2$$

est composé. On trouve

$$xz + yt = 14, \qquad xt - yz = 5,$$
$$xz - yt = 10, \qquad xt + yz = 11,$$

d'où

$$xz = 12, \qquad yt = 2, \qquad xt = 8, \qquad yz = 3,$$

$$\frac{xz}{yz} = \frac{12}{3} = \frac{4}{1},$$

d'où

$$x = 4, \qquad y = 1. \qquad x^2 + y^2 = 17 \qquad \text{et} \qquad 221 = 17.13.$$

4° Le nombre

$$N = a^4 + 4b^4 = (a^2 - 2b^2)^2 + 4a^2b^2$$

est une somme de deux carrés de deux façons différentes. On

aura

$$xz + yt = a^2, \qquad xt - yz = 2b^2,$$
$$xz - yt = a^2 - 2b^2, \qquad xt + yz = 2ab,$$

d'où

$$xz = a^2 - b^2, \quad yt = b^2, \quad xt = ab + b^2, \quad yz = ab - b^2,$$
$$\frac{xz}{yz} = \frac{a^2 - b^2}{ab - b^2} = \frac{a+b}{b};$$

d'où

$$x = a + b, \qquad y = b,$$

et

$$z = a - b, \qquad t = b$$

les deux facteurs sont

$$x^2 + y^2 = a^2 + 2ab + 2b^2, \qquad z^2 + t^2 = a^2 - 2ab + 2b^2$$

et

$$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2) \quad \text{(Sophie Germain)}$$

avec

$$a = 1, \qquad b = 2^n;$$

il vient

$$2^{4n+2} + 1 = (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1) \quad \text{(Aurifeuille).}$$

On peut, dans le même but, se servir d'une forme quadratique quelconque $x^2 + Dy^2$.

Partant de l'identité

$$(a^2 + Db^2)(c^2 + Dd^2) = (ac \pm Dbd)^2 + D(ad \mp bc)^2,$$

on trouvera les facteurs chaque fois qu'on aura une double représentation du nombre donné.

Ce procédé convient surtout quand on possède déjà une représentation quadratique.

4. On peut aussi se servir de la réciproque du théorème de Fermat.

Si l'on constate que la congruence $a^{N-1} \equiv 1 \pmod{N}$ n'est pas vérifiée, le nombre N est certainement composé.

Si cette congruence est vérifiée sans qu'elle le soit pour un sous-multiple de $N - 1$, le nombre N est premier.

On voit de suite le point faible de cette méthode.

Après avoir fait des opérations compliquées, on est souvent peu avancé, étant donné que si la congruence en question n'est pas satisfaite, on ne connaît pas les facteurs, et, si elle l'est, il est difficile de s'assurer qu'elle ne l'est pas pour un sous-multiple de N — 1.

Cependant, dans le cas de $N = 2^{2^n} + 1$ et $a = 3$, la méthode est infaillible, car

$$\left(\frac{3}{N}\right) = -1;$$

donc, si N est premier, on aura

$$3^{\frac{1}{2}(N-1)} \equiv -1 \pmod{N}$$

sans que cette relation puisse être vérifiée par un sous-multiple de (N — 1), les seuls sous-multiples étant dans ce cas 2^{2^k} avec $k < n$.

C'est ainsi que Morehead et Western (1909) ont prouvé que les nombres

$$N = F_7 = 2^{2^7} + 1 \qquad \text{et} \qquad N = F_8 = 2^{2^8} + 1$$

respectivement de 39 et 77 chiffres sont composés, puisque la congruence

$$3^{\frac{1}{2}(N-1)} \equiv -1 \pmod{N}$$

n'est pas vérifiée.

5. Passons à la décomposition par la forme $x^2 - y^2 = N$. La première question qui se pose est de savoir laquelle des inconnues sera trouvée directement par tâtonnement, l'autre pouvant être déterminée par les opérations directes. Si, par exemple, on connaît y, on aura $x = \sqrt{N + y^2}$. De même, si l'on connaît x, on aura $y = \sqrt{x^2 - N}$.

Remarquons d'abord que nous faisons abstraction de la solution évidente :

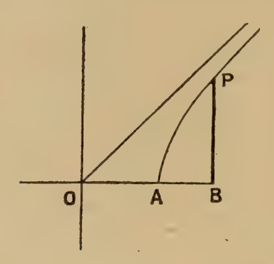
$$x = \frac{N+1}{2}, \qquad y = \frac{N-1}{2},$$

qui correspond à la décomposition non moins évidente, $N = 1.N$.

On aura toujours $y < x$ et il semble qu'il soit plus commode de

prendre y comme inconnue devant être trouvée directement par tâtonnement. Tel n'est pas le cas.

On peut le prouver sans calcul, en considérant la branche de l'hyperbole équilatère représentée par l'équation $x^2 - y^2 = N$.



Si P est un point entier de l'hyperbole (c'est-à-dire un point dont les coordonnées sont des nombres entiers), on aura

$$x = OB, \qquad y = BP.$$

Or, y peut assumer toutes les valeurs comprises entre O et BP, tandis que x ne peut assumer que des valeurs comprises entre OA et OB et l'on aura évidemment $AB < PB$.

Comme la Géométrie est étrangère à l'Arithmétique, nous allons donner une démonstration directe de ce qu'on aura moins de valeurs à essayer pour x que pour y.

Soient a et b les deux limites entre lesquelles on se propose de situer le plus petit facteur $a < b < \sqrt{N}$.

Comme le produit de ces facteurs est constant (N), la somme de ces facteurs est minimum quand les facteurs sont égaux, et croît au fur et à mesure que ces facteurs s'écartent l'un de l'autre.

On aura donc

$$\frac{1}{2}\left(b + \frac{N}{b}\right) < x < \frac{1}{2}\left(a + \frac{N}{a}\right)$$

et, puisque $a < x - y < b$,

$$\frac{1}{2}\left(\frac{N}{b} - b\right) < y < \frac{1}{2}\left(\frac{N}{a} - a\right).$$

Le nombre des valeurs à essayer est la différence des deux limites

ou

$$\frac{1}{2}\left(a+\frac{N}{a}\right)-\frac{1}{2}\left(b+\frac{N}{b}\right)=\frac{(N-ab)(b-a)}{2ab} \text{ (pour } x\text{)},$$

$$\frac{1}{2}\left(\frac{N}{a}-a\right)-\frac{1}{2}\left(\frac{N}{b}-b\right)=\frac{(N+ab)(b-a)}{2ab} \text{ (pour } y\text{)}.$$

On réalise donc une économie de

$$\frac{(N+ab)(b-a)}{2ab}-\frac{(N-ab)(b-a)}{2ab}=(b-a) \text{ essais.}$$

Nous verrons, dans la suite, d'autres raisons pour préférer la recherche de la valeur de x plutôt que celle de y.

6. Avant d'aller plus loin, remarquons qu'il est parfois préférable d'introduire un nouveau facteur et considérer la décomposition de $nN = x^2 - y^2$, le facteur n devant être convenablement choisi. Le but de l'introduction de ce facteur est de rapprocher les deux facteurs et, partant, de diminuer le nombre des essais à faire.

Soit, comme précédemment,

$$a < x - y < b < \sqrt{N}.$$

On aura pour x les limites

$$\frac{1}{2}\left(b+\frac{N}{b}\right) < x < \frac{1}{2}\left(a+\frac{N}{a}\right),$$

d'où

$$\frac{1}{2}\left(a+\frac{N}{a}\right)-\frac{1}{2}\left(b+\frac{N}{b}\right)=\frac{(N-ab)(b-a)}{2ab}$$

valeurs de x à essayer.

Considérons le nombre

$$nN = x_1^2 - y_1^2 = n(x^2 - y^2)$$

avec les limites

$$na < n(x-y) < nb < \sqrt{nN},$$

d'où

$$\frac{1}{2}\left(kb+\frac{N}{b}\right) < x_1 < \frac{1}{2}\left(ka+\frac{N}{a}\right)$$

et, par conséquent,

$$\frac{1}{2}\left(ka+\frac{N}{a}\right)-\frac{1}{2}\left(kb+\frac{N}{b}\right)=\frac{(N-kab)(b-a)}{2ab}$$

valeurs de x_1 à essayer.

Il en résulte une économie de

$$\frac{(N-ab)(b-a)}{2ab}-\frac{(N-kab)(b-a)}{2ab}=\frac{1}{2}(b-a)(k-1) \text{ essais.}$$

Toutefois, dans le choix de n, il est nécessaire de tenir compte de la relation

$$na < n(x-y) < nb < \sqrt{n}\,N \qquad \text{ou} \qquad nab < N.$$

Il est à remarquer que l'économie de $\frac{1}{2}(b-a)(k-1)$ essais est payée relativement cher, car on aura à opérer sur de plus grands nombres. En définitive, l'introduction d'un nouveau facteur n'est justifiée que rarement.

7. Supposons qu'il s'agisse d'un nombre de la forme $a^n \pm b^n$ dont les facteurs sont de la forme $kn+1$.

On aura donc

$$N = x^2 - y^2$$

et

$$x+y \equiv 1 \pmod{n},$$
$$x-y \equiv 1,$$

le module n étant supposé impair, d'où

$$x \equiv 1, \qquad y \equiv 0 \pmod{n}.$$

Ainsi x est limité à un cas sur n cas possibles, ainsi que y.

Mais $y \equiv 0 \pmod{n}$ donne

$$y^2 \equiv 0 \pmod{n^2}.$$

Cette valeur portée dans $x^2 - y^2 = N$ donne

$$x^2 \equiv N \pmod{n^2}, \qquad \text{d'où} \qquad x \equiv \pm r \pmod{n^2}.$$

Cette relation, jointe à la précédente $x \equiv 1 \pmod{n}$, donnera *une* solution et x serait limité à un cas sur n^2 cas possibles, tandis que y ne serait limité qu'à un cas sur n cas possibles.

Exemple. — $N = 2^{61} + 2^{31} + 1$ est facteur de $2^{122} + 1$. Posons $N = x^2 - y^2$, on a

$$N \equiv 1 + 36.61 \pmod{61^2 = 3721},$$
$$x \equiv 1 + 18.61 \pmod{3721} \quad y \equiv 0 \pmod{61}.$$

Supposons enfin qu'on ait établi

$$x \equiv 1 \pmod{2^n},$$
$$y \equiv 0,$$

la relation $y \equiv 0 \pmod{2^n}$ donne

$$y^2 \equiv 0 \pmod{2^{2n}},$$

d'où

$$x^2 \equiv N \pmod{2^{2n}} \quad \text{ou} \quad x \equiv \pm r \pmod{2^{2n-1}}.$$

Cette relation avec celle qui est indiquée plus haut

$$x \equiv 1 \pmod{2^n}$$

donne *une* solution $\pmod{2^{n-1}}$ et x serait limité à un cas sur 2^{2n-1} cas, tandis que y serait limité à un cas sur 2^n cas.

Exemple. — $2^{68} + 1$ est divisible par $17^2 = 289$. Le quotient est

$$N = 1\,021\,273\,028\,302\,258\,913 = x^2 - y^2;$$

on a

$$N \equiv 1 + 9.17 \pmod{17^2 = 289} \equiv 225 \pmod{256},$$

les deux facteurs devant être $x \equiv +1 \pmod{272}$ (V, **24**).

Si l'on pose

$$x + y = 16k + 1,$$
$$x - y = 16l + 1,$$

on aura

$$256kl + 16(k + l) + 1 = 225 - 256m.$$

Il en résulte que $k + l$ est pair et par conséquent $k - l$ aussi, d'où

$$2y = 16(k - l) \quad \text{donne} \quad y \equiv 0 \pmod{16}.$$

Ainsi on aura

$$y^2 \equiv 0 \pmod{256}, \quad \text{d'où} \quad x^2 \equiv N\ (256),$$

d'où

$$x \equiv \pm 15 \pmod{128}, \quad x \equiv 1 \pmod{8}.$$

Cette relation et celle trouvée précédemment donnent

$$x \equiv +113 \quad (\text{mod } 128).$$

On aura ainsi

$$x \equiv 1 + 13.17 \ (\text{mod } 17^2) \equiv 113 \ (\text{mod } 256)$$

ou

$$x \equiv 14961 \quad (\text{mod } 36992).$$

Ainsi x est limité à un seul cas sur 36992 cas possibles; y aurait été limité à un cas sur $17 \times 16 = 272$ cas possibles.

Ces considérations confirment notre affirmation qu'il est préférable de prendre x comme inconnue devant être trouvée par tâtonnement.

8. Par les considérations précédentes, nous sommes ainsi amenés à chercher une valeur de x satisfaisant à l'équation $x^2 - y^2 = N$. Cela revient à dire qu'il faut trouver entre certaines limites une valeur de x rendant $x^2 - N$ carré parfait.

Si l'on prend un module quelconque P et qu'on donne à x toutes les valeurs possibles pour ce module, si l'on calcule les valeurs correspondantes de y^2, on trouve une série de valeurs dont certaines seront résidus quadratiques, certaines autres non-résidus (mod P). Si une valeur quelconque de x donne pour y un non-résidu, cela prouve que cette valeur de x est inadmissible. Par là même, on éliminera certaines valeurs de x et l'on gardera les seules valeurs de x qui donnent pour y^2 un résidu.

Exemple. — Prenons, pour le module, le nombre 13 et supposons qu'on ait $N \equiv 10 \ (\text{mod } 13)$. Si l'on fait

$$x = \pm 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \qquad (\text{mod. } 13)$$

on obtient

$x^2 =$	0	1	4	9	3	12	10
$y^2 = x^2 - 10 =$	3	4	7	12	6	2	0
	r	r	n	r	n	n	

Ainsi, seules les valeurs $x \equiv \pm 0.1.3.6 \ (\text{mod } 13)$ sont admissibles.

Les valeurs $x \equiv 2.4.5 \ (\text{mod } 13)$ sont à éliminer.

Si, avec $P = 13$, on a $N = 11$ (non-résidu), on aura

$x \equiv \pm$	0	1	2	3	4	5	6	(mod 13)
$x^2 \equiv$	0	1	4	9	3	12	10	
$y^2 = x^2 - 11 \equiv$	2	3	6	11	5	1	12	
	n	*r*	*n*	*n*	*n*	*r*	*r*	

et

$$x \equiv \pm 1.5.6 \quad (\text{mod } 13)$$

sont les valeurs admissibles et

$$x \equiv \pm 0.2.3.4 \quad (\text{mod } 13)$$

sont à rejeter.

Chaque fois que N est un résidu pour le module considéré, il existe une valeur de x qui correspond à $y \equiv 0$. Dans ce cas, l'élimination peut être poussée plus loin.

Ainsi, dans le cas envisagé précédemment,

$$P = 13 \quad \text{et} \quad N \equiv 10 \quad (\text{mod } 13),$$

on aura pour x les solutions

$$x \equiv \pm 0.1.3.6 \quad (\text{mod } 13).$$

Les solutions $x \equiv \pm 0.1.3$ (mod 13) donnant pour y une valeur différente de 0 (mod 13) ne peuvent plus être réduites. Mais les solutions $x \equiv \pm 6$ (mod 13) donnant $y \equiv 0$ peuvent être réduites.

Soit, pour fixer les idées,

$$N \equiv 10 \quad (\text{mod } 13) \quad \text{avec} \quad N \equiv 75 \quad (\text{mod } 169).$$

Si l'on développe la solution $x \equiv \pm 6$ (mod 13) pour le module 169, on obtient :

$$x \equiv \pm \; 16.\; 7.19.\; 20.\; 32.33.\; 45.46.\; 58.\; 59.\; 71.\; 72.\; 84 \quad (\text{mod } 169),$$
$$x^2 \equiv + \; 35.49.23.\; 62.\; 10.75.166.88.153.101.140.114.127,$$
$$y^2 = x^2 - 75 \equiv 130.26.52.156.104.\; 0.\; 91.13.\; 78.\; 21.\; 65.\; 39.\; 52.$$

Toutes les valeurs de y^2 sont $\equiv 0$ (mod 13), mais seul

$$y^2 \equiv 0 \quad (\text{mod } 169)$$

peut devenir un carré. Il en résulte que des solutions

$$x \equiv \pm 6 \quad (\text{mod } 13)$$

seules les solutions $x \equiv \pm 33 \pmod{169}$ sont admissibles et les formes linéaires de x sont

$$x \equiv \pm 0.1.3 \pmod{13} \quad \text{ou} \quad \pm 33 \pmod{169}.$$

Il est cependant à remarquer que l'utilisation des modules P^2 ne peut être justifiée que pour les petites valeurs de P et lorsque les limites des valeurs de x sont très grandes.

9. Considérons en premier lieu le module 2^n.

Soit posé $N = x^2 - y^2$. Il est évident que si $N \equiv 1 \pmod 4$, x est impair et si $N \equiv 3 \pmod 4$, x est pair.

Ce dernier cas se subdivise en deux suivant que $N \equiv 3$ ou $7 \pmod 8$:

Si $N \equiv 3 \pmod 8$, on aura $x \equiv 2 \pmod 4$,
» 7 » 0 »

Aucune réduction ultérieure n'est plus possible, étant donné que, dans ce cas, y est différent de $0 \pmod{2^n}$.

Mais le cas de $N \equiv 1 \pmod 4$ donne lieu à des réductions plus importantes. D'abord, dans le cas de $N \equiv 5 \pmod 8$,

Si $N \equiv 5 \pmod{32}$, on aura $x \equiv \pm 3 \pmod{16}$
» 13 » 7 »
» 21 » 5 »
» 29 » 1 »

sans réduction ultérieure.

Mais, dans le cas de $N \equiv 1 \pmod 3$, la réduction peut être poursuivie plus loin de manière à obtenir finalement 2 cas sur 64, 2 cas sur 256, 2 cas sur 1024, etc., soit à la limite à

$$\frac{1}{32}\left(1 + \frac{1}{4} + \frac{1}{16} \cdots\right) = \frac{1}{32}\,\frac{4}{3} = \frac{1}{24}$$

de tous les cas possibles, c'est-à-dire 1 cas sur 24.

10. Considérons en second lieu le module 3.

Si $N \equiv 1$, on aura $x \equiv \pm 1$;
» 2 » 0.

Le deuxième cas est irréductible puisque y est différent de o (mod 3); mais le premier cas donne :

Si $N \equiv 1 \pmod 9$, on aura $x \equiv \pm 1$;
» 4 » 2;
» 7 » 4.

Dans ce cas, la réduction peut être poussée plus loin. Finalement, on aura dans ce cas : 2 cas sur 27, 2 cas sur 243, etc., ou à la limite :

$$\frac{2}{27}\,\frac{10}{9} = \frac{20}{243}.$$

Si, toutefois, on s'arrête au module 81, on aura 2 cas sur 27 et 2 cas sur 81, soit 8 cas sur 81.

11. Considérons le module 5 :

Si $N \equiv 2$, on aura $x \equiv \pm 1$;
» 3 » 2,

sans réduction ultérieure, puisque $y \not\equiv 0$.

Mais si $N \equiv 1$, on aura $x \equiv 0$ ou ± 1.
» 4 » 0 » ± 2.

La solution $x \equiv 0$ est irréductible; l'autre peut être ramenée à 2 cas sur 25 qui eux-mêmes peuvent être ramenés à 6 cas sur 125 ou à 4 cas sur 125 et 2 sur 625, etc.

Il en est de même des autres modules.

12. Afin de bien faire comprendre le procédé à suivre, nous allons refaire tous les calculs qui nous ont conduit à la décomposition d'un nombre de 19 chiffres.

On sait que

$$2^{122} + 1 = (2^{61} - 2^{31} + 1)(2^{61} + 2^{31} + 1).$$

On trouve

$$2^{61} - 2^{31} + 1 = 5.733.1709.368140581013,$$

$$2^{61} + 2^{31} + 1 = 2305843011361177601 = N.$$

C'est ce dernier nombre qui a échappé aux investigations de Lucas que nous allons décomposer.

Nous avons construit encore en 1914-1918 une Table donnant la plus petite solution de $2^x \equiv 1 \pmod{P}$ pour toutes les valeurs de P inférieures à 300000 ([1]). On trouve, par exemple, dans cette Table :

$$P = 733, \qquad x = 244,$$
$$P = 1709, \qquad x = 244;$$

donc 733 et 1709 divisent $2^{244} - 1$ ou $2^{122} + 1$.

En effet, ces facteurs divisent $2^{61} - 2^{31} + 1$, facteur de $2^{122} + 1$. On ne trouve point d'autre facteur de $2^{244} - 1$, donc de $2^{122} + 1$, donc de $2^{61} + 2^{31} + 1$, ce qui prouve que N n'a point de facteur < à 300000.

En prenant

$$N = 2^{61} + 2^{31} + 1 = a^2 - b^2,$$

on aura

$$\sqrt{N} < a < \frac{1}{2}\left(3 \times 10^5 + \frac{N}{300.000}\right)$$

ou

$$1518500250 < a < 3843071835601.$$

Ces résultats peuvent décourager plus d'une personne non habituée à ce genre de calcul; on a, en effet :

$$\begin{array}{r} 3843071835601 \\ -\ 1518500250 \\ \hline 3841553335351 \end{array}$$

nombres à considérer dont le plus petit est $\sqrt{N} = 1518500250$. A raison d'un nombre par seconde et 12 heures de travail par jour et 360 jours par an, ce travail demanderait :

$$\frac{384 \times 10^{10}}{60 \times 60 \times 12 \times 360} = 370.370 \text{ années.}$$

Et cependant nous allons le décomposer dans les quelques lignes qui suivent :

On a, en effet,

$$N = a^2 - b^2 \equiv 1 + 36 \times 61 \pmod{61^2} \equiv 1 \pmod{16} \equiv 2 \pmod{3};$$

([1]) *Voir* la note en bas de la page 126.

puisqu'on a $b \equiv 0 \pmod{61}$, on a

$$a \equiv +(1 + 18.61) \pmod{61^2}$$

D'autre part, les facteurs devant être de la forme $244k + 1$, on aura

$$a + b \equiv \pmod 4 \quad \text{ou} \quad a + b = 4k + 1,$$
$$a - b \equiv \qquad \text{ou} \quad a - b = 4l + 1$$

et

$$16kl + 4(K + l) + 1 \equiv 1 + 16n,$$

d'où $k + l =$ pair, de même que $k - l$. Il en résulte

$$b \equiv 0 \pmod 4 \quad \text{et} \quad a \equiv 1.$$

Mais $b \equiv 0 \pmod 4$ donne

$$b^2 \equiv 0 \pmod{16} \quad \text{et} \quad a^2 \equiv 1 \pmod{16},$$

d'où

$$a \equiv \pm 1 \pmod 8,$$

ce qui avec $a \equiv 1 \pmod 4$ donne

$$a \equiv +1 \pmod 8.$$

$N \equiv 2 \pmod 3$ donne

$$a \equiv 0 \pmod 3$$

sans réduction ultérieure.

Ainsi on a

$$a \equiv 1 + 18.61 \pmod{3721} \equiv 1 \pmod 8 \equiv 0 \pmod 3$$

ou

$$a \equiv 53193 \pmod{89304}.$$

Posons

$$a = 89304z + 53193;$$

cette valeur substituée dans

$$N < a < \frac{1}{2}\left(3 \times 10^5 + \frac{N}{3 \times 10^5}\right)$$

donne

$$17003 < z < 43033590.$$

Afin de ne pas commencer l'élimination à partir de 17003, remplaçons encore z par $17003 + x$. Il vient

$$a = 89304x + 1518578409 \quad \text{avec} \quad 0 < x < 43016587.$$

Avant d'aller plus loin, il est nécessaire de trouver les formes linéaires de x pour différents modules. De ces derniers, le module 3 est seul épuisé, puisque $a \equiv 0 \pmod 3$ et $b \not\equiv 0 \pmod 3$.

Commençons par le module 2^n. On a (mod 64) :

$$a \equiv 24x + 41 \quad \text{et} \quad N \equiv 1.$$

Posons :

$x =$	0	1	2	3	4	5	6	7	(mod 8)
$a \equiv 24x + 41 \equiv$	41	1	25	49	9	33	57	17	(mod 64)
$a^2 =$	17	1	113	97	81	65	49	33	(mod 128)
$b^2 = a^2 - 1 =$	16	0	112	96	80	64	48	32	»
$b^2 : 16 =$	1	0	7	6	5	4	3	2	(mod 8)
	r		n	n	n		n	n	

La forme linéaire $x \equiv 0 \pmod 8$ seule conduit à un résidu irréductible ; les formes linéaires $x \equiv 2.3.4.6.7$ conduisent aux non-résidus et doivent être rejetées. Les formes $x \equiv 1.5 \pmod 8$ peuvent être réduites.

Elles donnent :

$x \equiv$	1	5	9	13	17	21	25	29	(mod 32)
$a \equiv 216x + 233 \equiv$	193	33	129	225	65	161	1	97	(mod 256)
$a^2 \equiv$	385	65	257	449	129	321	1	193	(mod 512)
$b^2 \equiv a^2 - N \equiv a^2 - 1 \equiv$	384	64	256	448	128	320	0	192	(mod 512)
$b^2 : 64 \equiv$	6	1	4	7	2	5	0	3	(mod 8)
	n	r		n	n	n		n	

La forme linéaire $x \equiv 5 \pmod{32}$ conduit seule à un résidu irréductible, les formes linéaires

$$x \equiv 1.13.17.21.29 \pmod{32}$$

conduisent à un non-résidu ; les formes $x \equiv 9.25$ peuvent être réduites.

Pour ces dernières, on aura

$$x \equiv 9.25.41.57.73.89.105.121 \pmod{128}$$

dont la forme $x \equiv 73 \pmod{128}$ seule conduit à un résidu irréductible ; les formes $x \equiv 25.89 \pmod{128}$ peuvent être réduites ; les autres sont inadmissibles.

Les formes

$$x \equiv 25.89 \qquad (\text{mod } 128)$$

donnent

$$x \equiv 89.153 \qquad (\text{mod } 256).$$

Arrêtons-nous là. Nous aurons donc :

$$x \equiv 0 \ (\text{mod } 8) \ \text{ou} \ 5 \ (\text{mod } 32) \ \text{ou} \ 73 \ (\text{mod } 128) \ \text{ou} \ 89.153 \ (\text{mod } 256).$$

Considérons ensuite le module 5.

On a (mod 5) :

$x \equiv$	0	1	2	3	4
$a \equiv 4x + 4 \equiv$	4	3	2	1	0
$a^2 \equiv$	1	4	4	1	0
$b^2 \equiv a^2 - \text{N} \equiv a^2 - 1 \equiv$	0	3	3	0	1
		n	n		r

La forme linéaire $x \equiv 4$ (mod 5) seule conduit à un résidu irréductible ; les formes $x \equiv 1.2$ sont à rejeter. Les formes $x \equiv 0.3$ peuvent être réduites par le module 25 et deviennent

$$x \equiv 10.23 \qquad (\text{mod } 25).$$

Ces dernières peuvent à leur tour être réduites à 4 valeurs sur 125 et 2 sur 625.

On trouve

$$x \equiv 48.60.73.85 \quad (\text{mod } 125) \qquad \text{ou} \qquad 260.373 \quad (\text{mod } 625).$$

En résumé, les formes linéaires de x sont (mod 5^n) :

$$x \equiv 4 \quad (\text{mod } 5), \qquad 48.60.73.85 \quad (\text{mod } 125) \qquad \text{ou} \qquad 260.373 \quad (\text{mod } 625).$$

Considérons ensuite le module 7.

On a

$$\text{N} \equiv 5 \qquad \text{et} \qquad a = 5x + 5 \quad (\text{mod } 7).$$

Posons :

$x \equiv$	0	1	2	3	4	5	6	(mod 7)
$a = 5x + 5 \equiv$	5	3	1	6	4	2	0	
$a^2 \equiv$	4	2	1	1	2	4	0	
$b^2 \equiv a^2 - \text{N} \equiv a^1 - 5 \equiv$	6	4	3	3	4	6	2	
	n	r	n	n	r	n	r	

donc

$$x \equiv 1.4.6 \qquad (\text{mod } 7).$$

Ces formes ne donnent pas $b \equiv 0$ et ne peuvent être réduites (mod 49).

Le module 11 donne

$$N \equiv 5 \quad \text{et} \quad a \equiv 6x + 7.$$

Posons :

$x \equiv$	0	1	2	3	4	5	6	7	8	9	10	(mod 11)
$a \equiv 6x+7 \equiv$	7	2	8	3	9	4	10	5	0	6	1	
$a^2 \equiv$	5	4	9	9	4	5	1	3	0	3	1	
$b^2 \equiv a^2 - N \equiv$	0	10	4	4	10	0	8	9	7	9	8	
		n	r	r	n		n	r	n	r	n	

Donc les formes $x \equiv 2.3.7.9 \pmod{11}$ sont admissibles ; les formes $x \equiv 1.4.6.8.10 \pmod{11}$ sont à rejeter ; les formes $x \equiv 0.15$ peuvent être réduites par les modules 121 et donnent

$$x \equiv 11.38 \pmod{121}.$$

En continuant ainsi, on forme le Tableau suivant :

Décomposition de $N = 2^{61} + 2^{31} + 1 = 2305843011361177601 = a^2 - b^2$,

$$a = 89304x + 151857409 \qquad (0 < x < 43016587).$$

Mod.	N.	a.	x.
2^n	»	»	0 (mod 8), 5 (mod 32), 73 (mod 128), 89.153 (mod 256)
5^n	»	»	4 (mod 5), 48.60.73.85 (mod 125), 260.373 (mod 625)
7	5	$5x+5$	1.4.6
11	5	$6x+7$	2.3.7.9 (mod 11) ou 11.38 (mod 121)
13	1	$7x+10$	2.5.6.7.10 (mod 13) ou 47.56 (mod 169)
17	8	$3x+12$	1.3.6.8.12.13.14 (mod 17) ou 204.264 (mod 289)
19	18	$4x+8$	4.5.7.8.10.11.16.17.18.
23	2	$18x+5$	3.4.6.7.8.17.18.19.21.22 (mod 23) ou 46.48 (mod 529)
29	12	$13x+21$	0.1.2.6.7.10.11.17.18.21.22.26.27.28.
31	5	$24x+9$	0.2.5.7.9.11.12.15.16.17.21.22.23.26.27.29.
37	6	$23x+26$	0.1.3.6.8.9.10.12.13.14.18.21.25.28.32.33.34.36.
41	1	$6x+32$	0.1.2.3.6.11.12.13.15.18.19.20.22.24.25.26.29.31. 32.33.38.
47	30	$4x+43$	1.3.8.9.13.14.15.17.20.21.23.24.25.26.28.29.32. 34.35.36.40.41.46.
53	4	$52x+43$	0.1.3.5.6.10.11.14.15.16.17.18.19.22.23.27.28.30. 32.33.34.35.41.43.45.51.52.
59	5	$37x+6$	1.6.10.12.16.21.23.24.25.28.29.30.31.32.33.35,39. 40.41.42.46.48.49.50.51.52.53.56.57.58.

Pour se servir du module 61, il est nécessaire d'opérer de la façon suivante :

On a $b^2 = a^2 - N$ ou, en posant $b = 4.61.y$,

$$(244y)^2 = (89304x + 1518578409)^2 - (2^{61} + 2^{31} + 1)$$

ou

$$y^2 = 133956x^2 + 4555735227x + 3987048505$$

ou

$$(\text{mod } 61) \qquad y^2 \equiv 3x + 55,$$

d'où

$$x \equiv 1.2.3\ 5.6.7.11.14.15.16.17.18.21.22.24.27.29.36.38.41.43.44.47.48.49.50.51.54.58.59.60.$$

Étant donné que le champ de variation de x est très grand

$$(0 < x < 43016587),$$

on procédera par plusieurs étapes de la façon suivante :

1° On cherchera une solution :

$$x \equiv 89.153 \pmod{256} \equiv 4 \pmod{5}.$$

On trouvera qu'un seul nombre $x = 834649$ satisfait à toutes les conditions requises, mais à cause de $x \equiv 17 \pmod{289}$, il ne convient pas.

2° On cherchera une solution :

$$x \equiv 89.153 \pmod{256} = 48.60.73.85 \pmod{125}.$$

Aucune valeur de x ne satisfait à toutes les conditions.

3° Aucune valeur ne donne

$$x \equiv 89.153 \pmod{256} \equiv 260.373 \pmod{625}$$

avec toutes les autres conditions.

4° Aucune valeur ne donne

$$x \equiv 73 \pmod{128} \equiv 4 \pmod{5}$$

avec toutes les autres conditions.

5° Aucune valeur ne donne

$$x \equiv 73 \pmod{128} \equiv 48.60.73.85 \pmod{125}$$

avec toutes les autres conditions.

6° Aucune valeur ne donne

$$x \equiv 73 \pmod{128} \equiv 260.373 \pmod{625}$$

avec toutes les autres conditions.

7° On cherchera ensuite une solution

$$x \equiv 5 \pmod{32} \equiv 4 \pmod{5}.$$

On trouvera une seule valeur satisfaisant à toutes les conditions requises : c'est

$$x = 6\,789\,829.$$

8° On cherchera une solution

$$x \equiv 5 \pmod{32} \equiv 48.60.73.85 \pmod{125}.$$

On trouvera deux valeurs : $x \equiv 6931173,\ 10163173$, qui satisfont à toutes les conditions requises, dont la deuxième donne $x \equiv 25 \pmod{529}$ et ne convient par conséquent pas.

9° On ne trouvera aucune solution donnant

$$x \equiv 5 \pmod{32} \equiv 260.373 \pmod{625}.$$

10° On trouvera une solution

$$x \equiv 0 \pmod{8} \equiv 260.373 \pmod{625}$$

et c'est la valeur

$$x = 3\,717\,760.$$

11° On ne trouvera aucune solution

$$x \equiv 0 \pmod{8} \equiv 48.60.73.85 \pmod{125}.$$

12° On trouvera cinq solutions

$$x \equiv 0 \pmod{8} \equiv 4 \pmod{5};$$

ce sont

$$x \equiv 683624, \quad 12026384, \quad 5858624, 3\,923784, \quad 10238664$$

Ainsi on a huit nombres qui satisfont à toutes les conditions imposées.

La recherche de ces valeurs se fait par le procédé graphique que nous avons indiqué dans le troisième Chapitre.

Pour ne pas être obligé de vérifier les huit valeurs, on continuera l'élimination par les autres modules supérieurs à 61, mais sans chercher toutes les formes linéaires qui sont admissibles pour ces modules. On procédera de la façon suivante :

On a

$$x = 6789829,\quad 6931173,\quad 3717760,\quad 683624,\quad 12026384,\quad 5858624,\quad 3923784,\quad 10238664,$$

ou (mod 67) :

$x \equiv$	49	23	64	23	18	10	63	59
$a = 60x + 26 \equiv$	18	66	47	66	34	23	54	15
$a^2 \equiv$	56	1	65	1	17	60	35	24
$b^2 = a^2 - N \equiv a^2 - 28 \equiv$	28	40	37	40	56	32	7	63
	n					n	n	n

Il reste les quatre valeurs :

$$x = 6931173,\quad 3717760,\quad 683624,\quad 12026384$$

donnant (mod 71) :

$x \equiv$	11	58	36	49
$a = 57x + 21 \equiv$	9	61	14	45
$a^2 \equiv$	10	29	54	37
$b^2 \equiv a^2 - N \equiv a^2 - 60 \equiv$	21	40	65	48
	n		n	

Il ne reste que les deux valeurs $x = 3717760$ et 12026384 qui résistent aux modules 73 aussi. La seconde aurait été éliminée par les modules supérieurs à 73 ; la première donne :

$$x = 3717760,\qquad a = 89\,304x + 1\,518\,578\,409 = 333\,529\,417\,449,$$
$$a^2 = 111\,241\,872\,303\,869\,305\,667\,601,\quad N = 2\,305\,843\,011\,361\,177\,601,$$
$$b^2 = 111\,239\,566\,460\,857\,944\,490\,000 = 333\,525\,960\,700^2.$$

Ainsi :

$$\begin{aligned} a &= 333\,529\,417\,449 \\ b &= 333\,525\,960\,700 \\ \hline a + b &= 667\,055\,378\,149 \\ a - b &= 3\,456\,749 \end{aligned}$$

et

$$N = 2^{61} + 2^{31} + 1 = 3456749 \times 667055378149.$$

Nous avons trouvé de la même façon

$$2^{53} + 2^{27} + 1 = 15358129 \times 586477649$$

et

$$\frac{1}{9}(10^{19} - 1) \equiv 1111111111111111111$$

est premier.

13. Il est peut-être intéressant de comparer le progrès réalisé par le problème de factorisation avec le progrès des Tables des nombres premiers. Euler n'avait à sa disposition qu'une Table des nombres premiers jusqu'à 100000. Aussi ne s'attaque-t-il que rarement aux nombres de 9-10 chiffres et encore dans des cas spéciaux.

C'est Euler qui a donné le plus grand nombre premier connu à cette époque $2^{31} - 1$. C'est encore lui qui a décomposé

$$2^{32} + 1 = 641 \times 6700417$$

infirmant l'assertion de Fermat.

Au XIXe siècle, on a fait des Tables des nombres premiers jusque 10 millions et même au delà. Les procédés d'Euler deviennent insuffisants; et il est rarement avantageux de se servir de ces procédés, sauf, peut-être, quand il s'agit d'un nombre excédant peu la limite des Tables, de 9 ou 10 chiffres. Mais s'il s'agit d'un nombre de 12-13 chiffres, seul le procédé indirect par décomposition en $x^2 - y^2$ est pratique.

Si le nombre est d'une forme spéciale (diviseur de $a^n \pm b^n$), on peut encore s'attaquer à un nombre de 18-20 chiffres. Le nombre $2^{61} + 2^{31} + 1$, précédemment étudié, en fournit un exemple.

Mais la Science ne possède pas aujourd'hui une méthode pratique pour factoriser un nombre quelconque de 25-30 chiffres.

Pour ces nombres, on ne peut — et encore dans des cas exceptionnels — qu'être fixé sur la primalité ou non-primalité de ces nombres et encore sans avoir les facteurs dans le cas d'un nombre composé.

Nous avons cité des exemples : $2^{127} - 1$ est premier; $2^{128} + 1$ ainsi que $2^{256} + 1$ sont composés. Ces nombres sont respectivement de 39 et 77 chiffres.

TABLES

I. — Tables donnant les carrés de tous les nombres inférieurs à un million.

TABLE I.

	0	1	2	3	4	5	6	7	8	9
0	–	1	4	9	16	25	36	49	64	81
1	100	121	144	169	196	225	256	289	324	361
2	400	441	484	529	576	625	676	729	784	841
3	900	961	1024	1089	1156	1225	1296	1369	1444	1521
4	1600	1681	1764	1849	1936	2025	2116	2209	2304	2401
5	2500	2601	2704	2809	2916	3025	3136	3249	3364	3481
6	3600	3721	3844	3969	4096	4225	4356	4489	4624	4761
7	4900	5041	5184	5329	5476	5625	5776	5929	6084	6241
8	6400	6561	6724	6889	7056	7225	7396	7569	7744	7921
9	8100	8281	8464	8649	8836	9025	9216	9409	9604	9801

Exemples. — 1° Carré d'un nombre inférieur à 100 :

Le résultat est donné directement par la Table I.
Ainsi $76^2 = 5776$.

2° Carré d'un nombre compris entre 100 et 10000 :

On divise le nombre en tranches de deux chiffres, la première tranche de gauche pouvant contenir un seul chiffre. On écrit les nombres de la deuxième Table correspondant à ces tranches en ne tenant pas compte des chiffres imprimés en gras, et en avançant le deuxième résultat de deux chiffres. On fait la somme de ces résultats et l'on en soustrait le carré de la différence de deux tranches, reculé de deux chiffres.

Ainsi soit à trouver $43\,72^2$:

Première tranche 43	18 67 49
Deuxième tranche 72.........	52 35 84
	19 19 84 84
Carré de 72 — 43 = 29..	8 41
$4372^2 =$	19 11 43 84

3° Carré d'un nombre compris entre 10000 et 1000000 :

On divise le nombre donné en tranches de deux chiffres, en commençant par la droite, la première tranche de gauche pouvant contenir un seul chiffre.

TABLE II.

	0	1	2	3	4	5	6	7	8	9
0	00 00 00	01 01 01	04 04 04	09 09 09	16 16 16	25 25 25	36 36 36	49 49 49	64 64 64	81 81 81
1	1 01 01 00	1 22 22 21	1 45 45 44	1 70 70 69	1 97 97 96	2 27 27 25	2 58 58 56	2 91 91 89	3 27 27 24	3 64 64 61
2	4 04 04 00	4 45 45 41	4 88 88 84	5 34 34 29	5 81 81 76	6 31 31 25	6 82 82 76	7 36 36 29	7 91 91 84	8 49 49 41
3	9 09 09 00	9 70 70 61	10 34 34 24	10 99 99 89	11 67 67 56	12 37 37 25	13 09 08 96	13 82 82 69	14 58 58 44	15 36 36 21
4	16 16 16 00	16 97 97 81	17 81 81 64	18 67 67 49	19 55 55 36	20 45 45 25	21 37 37 16	22 31 31 09	23 27 27 04	24 25 25 01
5	25 25 25 00	26 27 27 01	27 31 31 04	28 37 37 09	29 45 45 16	30 55 55 25	31 67 67 36	32 81 81 49	33 97 97 64	35 16 15 81
6	36 36 36 00	37 58 58 21	38 82 82 44	40 09 08 69	41 37 36 96	42 67 67 25	43 99 99 56	45 34 33 89	46 70 70 24	48 09 08 61
7	49 49 49 00	50 91 91 41	52 36 35 84	53 82 82 29	55 31 30 76	56 81 81 25	58 34 33 76	59 88 88 29	61 43 44 84	63 04 03 41
8	64 64 64 00	66 27 26 61	67 91 91 24	69 58 57 89	71 27 26 56	72 97 97 25	74 70 69 96	76 45 44 69	78 22 21 44	80 01 00 21
9	81 81 81 00	83 64 63 81	85 49 48 64	87 36 35 49	89 25 24 36	91 16 15 25	93 09 08 16	95 04 03 09	97 01 00 04	98 99 99 01

On écrit les résultats de la Table II correspondant à ces tranches, en avançant chaque fois de deux chiffres, et on en fait la somme.

De cette somme il faut soustraire :

1° Le carré de la différence entre la première et la deuxième tranche;

2° Le carré de la différence entre la première et la troisième tranche;

3° Le carré de la différence entre la deuxième et la troisième tranche;

en reculant chaque fois vers la gauche de deux chiffres.

Ainsi soit à trouver $65\,72\,39^2$:

Première tranche 39		15 36 36 21
Deuxième tranche 72		52 36 35 84
Troisième tranche 65		42 67 67 25
		43 20 18 97 20 21
Carré de 72 — 39 = 33.	1089	
Carré de 65 — 39 = 26.	676	
Carré de 72 — 65 = 7.	49	
		— 55 86 89
$65\,72\,39^2 =$		43 19 63 10 31 21

Ce mode de calcul est basé sur l'identité

$$(10000a + 100b + c)^2 = 10000.10101\,a^2 + 100.10101\,b^2 + 10101\,c^2 - 100(b-c)^2 - 10000(a-c)^2 - 1000000(a-b)^2.$$

II. — Diviseurs linéaires des formes quadratiques.

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
		1	4	+ 1
8	± 1	2	8	1 3
12	1	3	6	1
		$4 = a^2$		
10	1	5	20	1 3 7 9
24	1 5	6	24	1 5 7 11
28	1 3 9	7	14	1 9 11
		$8 = 2a^2$		
		$9 = a^2$		
40	1 3 9 13	10	40	1 7 9 11 13 19 23 37
44	1 5 7 9 19	11	22	1 3 5 9 15
		$12 = 3a^2$		
26	1 3 9	13	52	1 7 9 11 15 17 19 25 29 31 47 49
56	1 5 9 11 13 25	14	56	1 3 5 9 13 15 19 23 25 27 39 45
60	1 7 11 17	15	30	1 17 19 23
		$16 = a^2$		
34	1 9 13 15	17	68	1 3 7 9 11 13 21 23 25 27 31 33
				39 49 53 63
		$18 = 2a^2$		
76	1 3 5 9 15 17	19	38	1 5 7 9 11 17 23 25 35
	25 27 31			
		$20 = 5a^2$		
42	1 5 17	21	84	1 5 11 17 19 23 25 31 37 41 55 71
88	1 3 7 9 13 21	22	88	1 9 13 15 19 21 23 25 29 31 35 43
	25 27 29 39			47 49 51 61 71 81 83 85
92	1 7 9 11 13 15	23	46	1 3 9 13 25 27 29 31 35 39 41
	19 25 29 41 43			
		$24 = 6a^2$		
		$25 = a^2$		
104	1 5 9 11 17 19	26	104	1 3 5 7 9 15 17 21 25 27 31 35
	21 23 25 37 45 49			37 43 45 47 49 51 63 71 75 81 85 93
		$27 = 3a^2$		
		$28 = 7a^2$		
58	1 5 7 9 13 23	29	116	1 3 5 9 11 13 15 19 25 27 31 33
	25			39 43 45 47 49 53 55 57 65 75 79 81
				93 95 99 109
120	1 7 13 17 19 29	30	120	1 11 13 17 23 29 31 37 43 47 49 59
	37 49			67 79 101 113

$\left(\frac{D}{x}\right) = 1,\quad z^2 - Dy^2.$ MODULE.	$x.$	D.	$z^2 + Dy^2,\quad \left(\frac{-D}{x}\right) = 1.$ MODULE.	$x.$
124	± 1 3 5 9 11 15 23 25 27 33 41 43 45 49 55	31	62	+ 1 5 7 9 19 25 33 35 39 41 45 47 49 51 59
		$32 = 2a^2$		
66	1 17 25 29 31	33	132	1 7 17 19 23 25 29 37 41 43 47 49 59 65 71 79 97 101 119 127
136	1 3 5 9 11 15 25 27 29 33 37 45 47 49 55 61	34	136	1 5 7 9 19 23 25 29 31 33 35 37 39 43 45 49 59 61 63 67 71 79 81 83 89 95 109 115 121 123 125 133
140	1 9 13 17 19 23 29 31 33 43 59 67	35	70	1 3 9 11 13 17 27 29 33 39 47 51
		$36 = a^2$		
74	1 3 7 9 11 21 25 27 33	37	148	1 9 15 19 21 23 25 31 33 35 39 41 43 49 51 53 55 59 65 73 77 79 81 85 87 91 101 103 119 121 131 135 137 141 143 145
152	1 9 11 13 15 17 21 25 29 31 35 37 43 49 59 69 71 73	38	152	1 3 7 9 13 17 21 23 25 27 29 37 39 47 49 51 53 55 59 63 67 69 73 75 81 87 91 109 107 111 116 119 121 137 141 147
156	1 5 7 19 23 25 31 35 41 49 61 67	39	78	1 5 11 25 41 43 47 49 55 59 61 71
		$40 = 10a^2$		
82	1 5 9 21 23 25 31 33 37 39	41	164	1 3 5 7 9 11 15 19 21 25 27 33 35 37 45 47 49 55 57 61 63 67 71 73 75 77 79 81 95 99 105 111 113 121 125 133 135 141 147 151
168	1 11 13 17 19 25 29 41 47 53 61 79	42	168	1 13 17 23 25 29 31 41 43 55 55 59 61 67 71 83 89 95 103 121 131 149 159 163
172	1 3 7 9 13 17 19 21 25 27 39 41 49 51 53 55 57 63 71 75 81	43	86	1 9 11 13 15 17 21 23 25 31 35 41 47 49 53 57 59 67 79 81 83
		$44 = 11a^2$		
		$45 = 5a^2$		
184	1 3 5 7 9 15 21 25 27 35 37 41 45 49 53 59 61 63 73 75 79 81	46	184	1 5 9 11 19 21 25 31 37 39 41 43 45 47 49 51 53 55 61 67 71 73 81 83 87 91 95 99 105 107 109 119 121 125 127 149 151 155 157 167 169 171 177 181
188	1 9 11 15 17 19 21 23 25 31 35 37 39 43 49 53 61 65 67 81 87 89 91	47	94	1 3 7 9 17 21 25 27 37 49 51 53 55 59 61 63 65 71 75 79 81 83 89
		$48 = 3a^2$		
		$49 = a^2$		

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
		$50 = 2a^2$		
204	± 1 5 7 13 25 29 31 35 41 47 49 59 65 79 83 91	51	102	+ 1 5 11 13 19 23 25 29 41 43 49 55 65 67 71 95
		$52 = 13a^2$		
106	1 7 9 11 13 15 17 25 29 37 43 47 49	53	212	1 3 9 13 17 19 23 25 27 29 31 35 37 39 49 51 55 57 67 69 71 75 77 79 81 83 87 89 93 97 103 105 111 113 117 121 127 139 147 149 151 153 165 167 169 171 179 191 197 201 205 207
		$54 = 6a^2$		
220	1 3 9 13 17 19 23 27 39 47 49 51 57 67 69 73 79 81 89 103	55	110	1 7 9 13 17 31 43 49 57 59 63 69 71 73 81 83 87 89 91 107
		$56 = 14a^2$		
114	1 7 25 29 41 43 49 53 55	57	228	1 11 23 25 29 31 35 41 47 49 53 61 65 67 73 79 83 85 89 91 103 113 119 121 127 131 151 157 169 173 185 191 211 215 221 223
232	1 3 7 9 11 19 21 23 25 27 33 37 43 49 57 61 63 65 69 71 75 77 81 85 99 101 103 111	58	232	1 9 15 21 25 31 33 35 37 39 47 49 51 55 57 59 61 65 67 69 77 79 81 83 85 91 95 101 107 115 119 121 123 127 129 133 135 139 143 157 159 161 169 179 187 189 191 205 209 213 215 219 221 225 227 229
236	1 5 9 11 17 21 23 25 29 31 39 41 43 45 47 49 53 55 57 67 81 83 85 91 99 103 105 111 115	59	118	1 3 5 7 9 15 17 19 21 25 27 29 35 41 45 49 51 53 57 63 71 75 79 81 85 87 95 105 107
		$60 = 15a^2$		
122	1 3 5 9 13 15 19 25 27 39 41 45 47 49 57	61	244	1 5 7 9 11 13 23 25 31 35 41 43 45 49 51 55 57 59 63 65 67 71 73 77 79 81 87 91 97 99 109 111 113 115 117 121 125 137 139 141 143 149 151 155 159 161 169 175 191 197 205 207 211 215 217 223 225 227 229 241
248	1 9 13 15 19 21 23 25 29 33 35 37 41 49 51 53 55 59 61 67 77 79 81 85 97 107 113 117 119 121	62	248	1 3 7 9 11 13 21 25 27 29 33 37 39 41 43 47 49 53 61 63 71 75 77 81 83 85 87 91 95 97 99 103 111 113 115 117 121 123 129 139 141 143 147 159 169 175 179 181 183 189 191 193 197 203 213 225 229 231 233 243
		$63 = 7a^2$		
		$64 = a^2$		
130	1 7 9 29 33 37	65 (suite p. 167)	260	1 3 9 11 19 23 27 29 31 33 37 43

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
130	± 47 49 51 57 61 63	65 (suite)	260	+ 49 57 59 61 69 71 73 81 87 93 97 99
				101 103 107 111 119 121 127 129 137 147 151 171
				177 181 183 193 197 207 209 213 219 239 243 253
264	1 5 13 17 19 25	66	264	1 5 7 13 17 23 25 35 41 47 49 53
	31 41 43 49 53 59			61 65 67 71 79 83 85 91 97 107 109 115
	61 65 85 95 97 103			119 125 127 131 151 161 163 169 175 191 205 221
	109 125			227 233 235 245
268	1 3 7 9 11 17	67	134	1 9 15 17 19 21 23 25 29 33 35 37
	21 25 27 29 31 33			39 47 49 55 59 65 71 73 77 81 83 89
	37 43 49 51 63 65			91 93 103 107 121 123 127 129 131
	73 75 77 79 81 87			
	89 93 95 99 111 115			
	119 121 129			
		$68 = 17a^2$		
138	1 5 11 13 17 25	69	276	1 5 7 13 17 19 25 35 43 47 49 53
	31 49 55 55 65			59 65 67 71 73 79 85 89 91 95 103 113
				119 121 125 131 133 137 149 167 169 175 179 193
				199 215 221 235 239 245 247 265
280	1 3 9 11 17 23	70	280	1 9 17 19 33 37 39 43 47 53 59 61
	27 31 33 37 51 53			67 69 71 73 79 81 87 93 97 101 103 107
	61 69 73 81 83 93			121 123 131 139 143 151 153 163 167 169 171 181
	97 99 101 111 121 127			191 197 223 229 239 249 251 253 257 267 269 277
284	1 5 7 9 11 23	71	142	1 3 5 9 15 19 25 27 29 37 43 45
	25 29 31 35 37 39			49 57 73 75 77 79 81 83 87 89 91 95
	45 47 49 51 55 57			101 103 107 109 111 119 121 125 129 131 135
	59 63 67 73 77 81			
	89 99 101 109 115 121			
	123 125 127 129 139			
		$72 = 2a^2$		
146	1 3 9 19 23 25	73	292	1 7 9 11 15 25 31 37 39 41 43 47
	27 35 37 41 49 55			49 51 57 59 61 63 65 69 77 81 83 85
	57 61 65 67 69 71			87 89 95 97 99 103 105 107 109 115 121 131
				135 137 139 145 149 151 159 163 165 167 169 173
				175 179 181 191 199 201 213 217 221 225 237 239
				247 257 259 263 265 269 271 273 275 279 287 289
296	1 5 7 9 13 19	74	296	1 3 5 9 11 13 15 23 25 27 29 31
	25 29 33 35 41 43			33 39 41 45 49 55 61 65 67 69 73 75
	45 47 49 51 59 61			79 81 83 87 93 99 103 107 109 115 117 119
	63 65 69 71 73 81			121 123 125 133 135 137 139 143 145 147 155 165
	91 93 95 109 117 121			167 169 183 191 195 199 201 205 207 211 219 225
	125 127 131 133 137 145			233 237 239 243 245 249 253 261 275 277 279 289
		$75 = 3a^2$		

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
		$76 = 19a^2$		
154	± 1 9 13 15 17 19	77	308	+ 1 3 9 13 17 25 27 31 37 39 41 43
	23 25 37 41 53 61			47 51 53 59 61 73 75 79 81 93 95 101
	67 71 73			103 107 111 113 115 117 123 127 129 137 141 145
				151 153 159 169 173 177 183 199 211 219 221 223
				225 237 239 241 243 251 263 279 285 289 293 303
312	1 7 11 23 25 29	78	312	1 19 25 29 35 37 41 47 49 53 55 67
	31 37 41 43 49 53			71 77 79 85 89 101 103 107 109 115 119 121
	59 77 83 85 89 95			127 131 137 155 161 163 167 173 179 187 199 215
	101 109 121 137 139 151			217 229 239 251 253 269 281 289 295 301 305 307
316	1 3 5 7 9 13	79	158	1 5 9 11 13 19 21 23 25 31 45 49
	15 21 25 27 35 39			51 55 65 67 73 81 83 87 89 95 97 99
	43 45 47 49 59 63			101 105 111 115 117 119 121 123 125 129 131 141
	65 71 73 75 81 89			143 151 155
	91 97 101 103 105 107			
	117 121 125 127 129 135			
	139 141 147			
		$80 = 5a^2$		
		$81 = a^2$		
328	1 3 9 11 13 19	82	328	1 7 9 13 15 25 29 33 43 47 49 51
	23 25 27 29 31 33			53 55 57 59 63 69 71 73 79 81 83 85
	35 39 49 53 57 67			91 93 95 101 105 107 109 111 113 115 117 121
	69 73 75 81 85 87			131 135 139 149 151 155 157 163 167 169 175 181
	93 99 101 103 105 109			183 185 187 191 195 199 201 203 209 225 229 231
	113 117 119 121 127 143			239 241 251 253 261 263 267 283 289 291 293 297
	147 149 157 159			301 305 307 309 311 317 323 325
332	1 9 15 17 19 21	83	166	1 3 7 9 11 17 21 23 25 27 29 31
	25 29 33 35 37 39			33 37 41 49 51 59 61 63 65 69 75 77
	41 43 47 49 55 61			81 87 93 95 99 109 111 113 119 121 123 127
	65 67 69 71 77 79			131 147 151 153 161
	81 91 93 103 107 109			
	113 115 121 135 139 143			
	153 155 159 161 163			
		$84 = 21a^2$		
170	1 3 7 9 19 21	85	340	1 9 11 21 31 37 39 43 47 49 57 67
	23 27 37 49 57 59			69 71 73 79 81 83 87 89 91 97 99 101
	63 69 73 81			103 113 121 123 127 131 133 139 149 159 161 169
				173 177 183 189 193 197 199 203 211 223 229 231
				233 247 263 277 279 281 287 299 307 311 313 317
				321 327 333 337
344	1 5 7 9 11 17	86	344	1 3 5 9 15 17 19 23 25 27 29 31
	25 29 35 37 39 41			37 41 45 47 49 51 57 61 69 75 77 79

(suite p. 169)

$\left(\frac{D}{x}\right)=1$, z^2-Dy^2. MODULE.	x.	D.	z^2+Dy^2, $\left(\frac{-D}{x}\right)=1$. MODULE.	x.
344	± 45 49 55 57 59 61	86	344	+ 81 85 89 91 93 95 97 103 111 115 121 123
	63 67 69 71 77 81	(suite)		125 127 131 135 141 143 145 147 149 153 155 157
	83 85 93 97 99 107			163 167 169 171 179 183 185 193 205 207 211 225
	119 121 125 139 141 145			227 231 235 237 239 243 245 255 261 271 273 277
	149 151 153 157 159 169			279 281 285 289 291 305 309 311 323 331 333 337
348	1 13 17 19 23 25	87	174	1 7 11 13 17 25 41 47 49 67 77 89
	31 35 41 43 49 55			91 95 101 103 109 113 115 119 121 131 137 139
	59 71 77 79 83 89			143 151 155 169
	101 107 109 113 121 127			
	137 163 167 169			
		$88 = 22a^2$		
178	1 5 9 11 17 21	89	356	1 3 5 7 9 15 17 19 21 23 25 27
	25 39 45 47 49 53			31 35 43 45 49 51 53 57 59 63 69 73
	55 57 67 69 71 73			75 81 83 85 93 95 97 103 105 109 115 119
	79 81 85 87			121 125 127 129 133 135 143 147 151 153 155 157
				159 161 163 169 171 173 175 177 189 191 207 211
				215 217 219 225 233 239 243 245 249 255 257 265
				269 277 279 285 289 291 295 301 309 315 317 319
				323 327 343 345
		$90 = 10a^2$		
364	1 3 5 9 11 15	91	182	1 5 9 19 23 25 29 31 33 41 43 45
	25 27 29 33 41 45			47 51 53 59 73 79 81 83 89 95 97 107
	53 55 67 71 73 75			111 113 115 121 125 127 145 155 165 167 171 179
	81 87 89 97 99 103			
	113 121 123 125 131 135			
	139 145 151 159 163 165			
		$92 = 23a^2$		
186	1 7 11 17 19 23	93	372	1 17 25 29 35 43 47 49 53 55 59 65
	25 29 49 53 65 67			71 77 79 89 91 95 97 107 109 115 121 127
	77 83 89			131 133 137 139 143 151 157 161 169 185 191 193
				197 199 205 209 223 227 247 253 259 269 271 287
				289 299 305 311 331 335 349 353 359 361 365 367
376	1 3 5 9 13 15	94	376	1 5 7 9 11 13 17 19 25 29 35 43
	17 23 25 27 29 31			45 49 55 63 65 67 69 71 77 79 81 85
	39 45 49 51 59 65			89 91 93 95 97 99 103 107 109 111 117 119
	69 75 77 81 83 85			121 123 125 133 139 143 145 153 159 163 169 171
	87 89 93 97 109 115			175 177 179 181 183 187 191 203 209 211 215 219
	117 121 125 127 131 133			221 225 227 229 239 241 245 247 249 261 263 271
	135 145 147 151 153 155			275 289 293 301 303 315 317 319 323 325 335 337
	167 169 177 181			339 343 345 349 353 355 361 373
380	1 7 9 13 23 31	95	190	1 3 9 11 13 27 33 37 39 49 53 61
	33 37 43 47 49 51	(suite p. 170)		67 81 97 99 101 103 107 111 113 117 119 121

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
380	± 53 59 61 63 71 79	95	190	+ 127 131 139 143 147 149 159 161 167 169 173 183
	81 83 87 91 97 101	(suite)		
	113 117 121 123 149 151			
	161 163 169 173 179 187			
		$96 = 6a^2$		
194	1 3 9 11 25 27	97	388	1 7 9 15 19 23 25 33 39 49 51 53
	31 33 35 43 47 49			55 59 61 63 65 67 71 73 81 83 85 87
	53 61 65 73 75 79			89 93 101 105 107 109 111 113 121 123 127 129
	81 85 89 91 93 95			131 133 135 139 141 143 145 155 161 169 171 175
				179 185 187 193 197 199 205 207 211 215 221 223
				225 229 231 235 237 239 241 251 263 269 271 273
				285 289 293 297 309 311 313 319 331 341 343 345
				347 351 353 357 359 361 367 371 375 377 383 385
		$98 = 2a^2$		
		$99 = 11a^2$		
		$100 = a^2$		
202	1 5 9 13 17 19	101	404	1 3 5 7 9 11 13 15 17 21 25 27
	21 23 25 31 33 37			33 35 37 39 45 49 51 55 59 63 65 67
	43 45 47 49 65 71			75 77 81 83 85 91 97 99 103 105 111 117
	77 79 81 85 87 95			119 121 125 127 135 137 139 143 147 151 153 157
	97			163 165 167 169 175 177 181 185 187 189 191 193
				195 197 199 201 221 225 231 233 243 245 249 255
				259 263 271 273 275 281 289 291 295 297 309 311
				315 317 325 331 333 335 343 347 351 357 361 363
				373 375 381 385
408	1 7 11 19 25 31	102	408	1 23 25 35 37 41 49 53 55 59 61 65
	37 41 43 47 49 53			71 77 83 91 95 101 103 109 113 121 127 133
	61 65 67 77 79 101			139 143 147 149 151 155 163 167 169 179 181 203
	107 109 113 115 121 131			209 211 215 217 223 233 235 247 251 271 277 283
	133 145 149 169 175 181			293 301 311 319 329 335 341 361 365 377 379 389
	191 199			395 397 401 403
412	1 3 9 11 13 17	103	206	1 7 9 13 15 17 19 23 25 29 33 41
	25 27 29 31 33 35			49 55 59 61 63 67 81 83 91 93 97 105
	39 41 43 47 49 51			107 111 117 119 121 129 131 133 135 137 139 141
	61 67 71 75 81 87			149 153 155 159 161 163 167 169 171 175 177 185
	93 95 97 99 105 115			195 201 203
	117 121 123 127 129 133			
	137 141 143 147 149 151			
	153 161 169 183 185 187			
	191 199 201			
		$104 = 26a^2$		
210	1 13 23 41 53 59	105	420	1 11 13 19 31 41 43 47 53 57 71 73
		(suite p. 171)		

$\left(\frac{D}{x}\right) = 1,\quad z^2 - Dy^2.$							D.	$z^2 + Dy^2,\quad \left(\frac{-D}{x}\right) = 1.$												
MODULE.	x.							MODULE.	x.											
210	± 73	79	89	97	101	103	105	420	+ 83	89	97	101	109	113	121	127	137	139	143	157
							(suite)		163	167	169	179	191	197	199	209	227	233	239	247
									269	271	289	313	317	341	359	361	383	391	397	403
424	1	3	5	7	9	15	106	424	1	5	9	11	17	21	23	25	31	39	43	45
	17	19	21	25	27	35			49	55	57	59	61	73	79	81	85	87	89	91
	45	47	49	51	57	61			97	99	101	103	105	107	109	111	113	115	121	123
	63	67	75	81	83	85			125	127	131	133	141	151	153	155	157	163	167	169
	89	95	97	101	105	109			173	181	187	189	191	195	201	203	207	211	215	219
	113	119	121	125	133	135			225	227	231	239	241	245	247	249	253	259	263	275
	139	141	143	147	153	157			277	279	281	285	287	289	295	305	307	329	331	341
	169	171	173	175	179	181			347	349	351	355	357	359	361	373	377	383	387	389
	183	189	199	201					391	395	397	405	409	411	417	421				
428	1	7	9	13	15	25	107	214	1	3	9	11	13	19	23	25	27	29	33	35
	29	31	33	37	41	43			37	39	41	47	49	53	57	61	69	75	79	81
	49	51	53	55	57	59			83	85	87	89	99	101	105	111	117	119	121	123
	61	63	67	69	71	81			137	141	143	147	149	151	155	159	163	169	171	183
	85	89	91	95	101	103			191	197	199	207	209							
	105	115	117	121	127	131														
	135	137	139	141	149	167														
	169	175	179	187	191	193														
	195	197	203	209	211															
							$108 = 3a^2$													
218	1	3	5	7	9	15	109	436	1	5	9	11	19	21	23	25	29	39	45	47
	21	25	27	29	31	35			49	51	55	59	61	67	73	79	81	89	91	93
	43	45	49	61	63	71			95	97	99	105	107	111	113	115	119	121	123	125
	73	75	81	83	87	89			127	129	137	139	145	151	157	159	163	167	169	171
	93	97	105						173	179	189	193	195	197	199	207	209	213	219	221
									225	231	233	235	245	249	251	253	255	259	261	271
									275	281	283	287	289	293	295	301	303	305	319	333
									335	349	351	353	359	361	365	367	371	373	379	383
									393	395	399	401	403	405	409	419	421	423	429	433
440	1	9	17	21	23	29	110	440	1	3	7	9	17	19	21	27	29	31	37	39
	37	39	43	47	49	53			51	53	57	61	63	67	71	73	81	87	89	93
	57	59	61	73	79	81			101	109	111	119	127	131	133	139	147	149	153	157
	83	89	91	93	101	103			159	163	167	169	171	183	189	191	193	199	201	203
	107	109	123	133	149	151			207	211	213	219	233	243	259	261	263	267	279	289
	153	157	169	179	189	193			299	303	311	317	323	327	333	337	343	349	357	361
	201	207	213	217					371	381	393	397	399	401	417	427				
444	1	5	11	17	19	25	111	222	1	5	7	17	23	25	29	35	49	59	67	73
	29	31	43	47	49	55			85	89	113	115	119	121	125	127	131	139	143	145
	71	73	79	83	85	89			151	157	161	167	169	175	179	181	191	203	209	211
	91	95	103	107	113	121														

(suite p. 172)

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$.		D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$.	
MODULE.	x.		MODULE.	x.
444	±125 145 155 157 161 163	111		
	169 181 187 199 209 215	(suite)		
		$112 = 7a^2$		
226	1 7 9 11 13 15	113	452	+ 1 3 9 13 19 23 25 27 35 39 41 43
	25 31 41 49 51 53			47 49 53 55 57 59 61 67 69 71 75 77
	57 61 63 69 77 81			79 81 85 97 103 105 107 109 117 119 121 123
	83 85 87 91 95 97			129 141 145 147 149 151 155 157 159 165 167 169
	99 105 109 111			173 177 179 183 185 187 191 199 201 203 207 213
				217 223 225 231 233 237 241 243 247 255 257 259
				263 271 277 289 291 299 309 313 315 317 319 321
				325 327 337 341 351 353 357 359 361 363 365 369
				379 387 389 397 401 407 415 419 421 423 431 435
				437 441 445 447
456	1 5 7 11 13 25	114	456	1 5 13 23 25 31 37 41 43 47 49 59
	35 37 41 49 55 65			65 73 77 79 89 101 103 107 109 113 115 119
	67 71 73 77 83 89			121 125 127 139 149 151 155 163 169 179 181 185
	91 101 109 113 121 125			187 191 197 203 205 215 223 227 235 239 245 257
	131 143 149 167 169 175			263 281 283 289 295 299 311 313 319 325 359 365
	181 185 197 199 205 211			371 373 385 389 395 401 403 421 427 439 445 449
460	1 3 9 11 17 19	115	230	1 7 9 17 29 31 33 37 39 41 43 49
	27 29 33 37 41 47			53 57 59 63 67 71 81 83 97 101 103 107
	49 51 53 57 79 81			113 119 121 131 137 139 141 143 151 153 157 169
	87 91 97 99 101 111			179 183 203 209 211 217 219 227
	113 121 123 127 137 141			
	147 153 157 159 163 167			
	169 171 187 191 199 209			
	217 223			
		$116 = 29a^2$		
		$117 = 13a^2$		
472	1 3 9 13 17 19	118	472	1 7 9 11 13 15 17 25 37 41 43 49
	23 25 27 31 35 37			57 61 63 67 69 71 77 79 81 83 87 91
	39 41 47 49 51 55			93 95 99 101 105 109 115 117 119 121 127 131
	57 61 69 75 77 81			135 137 141 143 145 149 153 155 157 159 165 167
	93 101 103 105 107 109			169 173 175 179 187 193 195 199 211 219 221 223
	111 117 121 123 137 139			225 227 229 235 239 241 255 257 259 263 265 267
	141 145 147 149 151 153			269 271 275 281 283 287 289 291 301 309 311 321
	157 163 165 169 171 173			325 333 339 343 347 349 359 361 365 369 375 383
	183 191 193 203 207 215			387 397 399 407 417 419 421 425 427 433 437 439
	221 225 229 231			441 443 445 449 451 453 467 469
476	1 5 9 11 19 23	119	238	1 3 5 9 15 25 27 31 41 43 45 53
	25 39 41 45 47 53			61 67 73 75 81 93 97 121 123 125 127 129
	55 59 61 71 73 79	(suite p. 173)		131 135 137 139 143 149 151 155 159 167 169 173

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
476	± 81 83 87 93 95 97	119	238	+179 181 183 191 199 201 205 209 215 219 225 227
	99 103 107 111 115 121	(suite)		
	125 129 137 149 163 169			
	171 173 181 195 201 205			
	207 209 211 223 225 235			
		$120 = 30a^2$		
		$121 = a^2$		
488	1 9 11 15 21 25	122	488	1 3 7 9 19 21 23 25 27 29 31 37
	29 35 37 39 41 43			41 49 53 55 57 63 65 69 71 73 75 79
	47 49 51 53 57 59			81 83 85 87 93 97 101 107 111 113 121 123
	65 67 69 73 81 85			131 133 137 143 147 151 157 159 161 163 165 169
	91 93 95 97 99 101			171 173 175 179 181 187 189 191 195 203 207 213
	103 113 115 119 121 127			215 217 219 221 223 225 235 237 241 243 249 255
	133 135 137 139 155 157			257 259 261 277 279 283 287 289 291 295 303 311
	161 165 167 169 173 181			321 333 335 339 343 347 349 353 359 361 363 369
	189 195 211 213 217 221			371 373 379 383 385 389 393 397 399 411 421 429
	225 227 231 237 239 241			437 441 443 445 449 453 455 471 473 475 477 483
492	1 7 17 19 23 25	123	246	1 11 17 25 29 31 35 37 43 47 49 53
	29 37 49 53 55 59			61 65 71 73 89 91 95 101 103 115 121 127
	61 65 67 73 79 83			133 137 139 149 161 163 167 169 179 187 191 223
	89 101 107 119 121 131			227 233 239 241
	133 137 143 149 151 155			
	161 169 175 199 203 211			
	215 233 235 241			
		$124 = 31a^2$		
		$125 = 5a^2$		
		$126 = 14a^2$		
508	1 3 7 9 13 17	127	254	1 9 11 13 15 17 19 21 25 31 35 37
	21 23 25 27 37 39			41 47 49 61 69 71 73 79 81 87 99 103
	41 43 49 51 55 59			107 113 115 117 121 129 131 135 143 145 149 153
	61 63 67 69 73 75			157 159 161 163 165 169 171 177 179 187 189 191
	81 83 91 95 111 113			195 197 199 201 203 209 211 215 221 225 227 231
	117 119 121 123 129 139			247 249 251
	145 147 149 151 153 155			
	157 161 165 167 169 175			
	177 183 189 197 201 207			
	209 219 221 223 225 235			
	239 243 249			
		$128 = 2a^2$		
258	1 5 13 25 29 31	129	516	1 5 7 11 13 19 23 25 29 35 47 49
	49 65 67 71 77 79			55 59 65 77 83 89 91 95 97 107 109 113
	89 97 103 109 113 119			115 121 125 133 137 143 145 149 151 161 163 167
	121 125 127	(suite p. 174)		169 175 181 193 199 203 209 211 223 229 233 235

$\left(\frac{D}{x}\right) = 1, \quad z^2 - Dy^2.$							D.	$z^2 + Dy^2, \quad \left(\frac{-D}{x}\right) = 1.$												
MODULE.	x.							MODULE.	x.											
							129 (suite)	516	239	245	247	251	253	257	275	289	295	299	311	319
									325	329	331	337	343	359	361	377	385	389	397	413
									415	431	437	443	445	449	455	463	475	479	485	499
520	± 1	3	7	9	11	19	130	520	1	9	21	23	31	33	49	51	53	57	67	71
	21	27	33	43	47	49			73	77	81	83	87	97	103	109	111	119	121	123
	53	57	59	63	73	77			127	129	131	133	137	139	141	149	151	157	163	173
	79	81	97	99	107	109			177	179	183	187	189	193	203	207	209	211	227	229
	121	129	133	137	141	147			237	239	251	259	263	267	271	277	279	287	289	297
	149	157	159	167	171	173			301	303	307	319	321	323	329	339	349	353	359	361
	177	189	191	193	199	209			367	373	407	413	419	421	427	431	441	451	457	459
	219	223	229	231	237	243			461	473	477	479	483	491	493	501	503	509	513	517
524	1	5	9	13	19	21	131	262	1	3	5	7	9	11	13	15	21	25	27	33
	23	25	31	33	41	45			35	39	41	43	45	49	53	55	59	61	63	65
	47	49	51	53	61	65			75	77	81	89	91	99	101	105	107	109	113	117
	67	71	77	79	81	83			121	123	125	129	135	143	147	151	159	165	167	169
	87	89	95	101	103	105			175	177	179	183	189	191	193	195	205	211	215	225
	109	111	113	115	117	119			231	233	239	243	245							
	121	125	127	129	139	155														
	163	165	169	171	177	187														
	189	193	199	203	205	207														
	219	223	225	227	233	235														
	245	247	251	255	259															
							$132 = 33a^2$													
266	1	3	9	11	13	23	133	532	1	9	13	15	25	33	41	47	51	55	67	69
	25	27	31	33	39	41			71	79	81	83	85	87	89	93	97	107	111	115
	43	59	69	75	81	85			117	121	127	129	131	135	137	139	145	149	151	155
	89	93	97	99	103	117			159	169	173	177	179	181	183	185	187	195	197	199
	121	123	129						211	215	219	225	233	241	251	253	257	265	269	271
									277	283	289	293	295	297	303	305	309	311	319	325
									327	331	339	341	365	367	369	375	379	389	391	407
									409	419	423	429	431	433	457	459	467	471	473	479
									487	489	493	495	501	503	505	509	515	521	527	529
536	1	5	7	9	13	17	134	536	1	3	5	9	11	13	15	17	23	25	27	33
	19	25	31	33	35	45			39	43	45	47	49	51	53	55	61	65	69	71
	49	53	59	61	63	65			73	75	81	85	89	99	101	103	109	115	117	121
	69	73	79	81	83	85			125	127	129	133	135	139	141	143	147	151	153	159
	87	89	91	95	101	107			165	167	169	179	183	187	193	195	197	199	203	207
	109	111	117	119	121	123			213	215	217	219	221	223	225	229	235	241	243	245
	125	129	131	133	141	153			251	253	255	257	259	263	265	267	275	287	289	297
	155	163	165	169	171	175			299	303	305	309	325	327	331	345	347	351	355	359
	191	193	197	211	213	217			361	363	365	373	375	379	381	387	391	399	405	413
	221	225	227	229	231	239	(suite p. 175)		417	423	425	429	431	439	441	443	445	449	453	457

$\left(\frac{D}{x}\right) = 1,\quad z^2 - Dy^2.$		D.	$z^2 + Dy^2,\quad \left(\frac{-D}{x}\right) = 1.$	
MODULE	x.		MODULE.	x.
536	±241 245 247 253 257 265	134 (suite)	536	+459 473 477 479 495 499 501 505 507 515 517 529
		$135 = 15a^2$		
		$136 = 34a^2$		
274	1 7 9 11 15 17	137	548	1 3 9 17 23 25 27 31 35 37 43 47
	19 25 37 39 49 59			49 51 55 61 65 67 69 71 73 75 77 79
	61 63 65 69 73 77			81 83 91 93 95 101 105 109 111 121 127 129
	81 87 93 99 101 103			131 133 141 143 145 147 153 163 165 169 173 179
	105 107 109 115 119 121			181 183 191 193 195 197 199 201 203 205 207 209
	123 129 133 135			213 219 223 225 227 231 237 239 243 247 249 251
				257 265 271 273 279 281 285 287 289 293 295 303
				307 313 315 319 327 331 333 337 359 361 363 371
				373 377 381 387 389 391 393 397 399 409 413 423
				425 429 431 433 435 441 445 449 451 459 461 463
				485 489 491 495 503 507 509 515 519 527 529 533
				535 537 541 543
552	1 17 19 25 29 31	138	552	1 7 11 17 25 29 37 47 49 61 65 71
	35 37 43 49 55 59			73 77 79 83 89 95 101 103 107 109 113 119
	61 65 67 73 77 89			121 137 139 155 157 163 167 163 173 175 181 187
	91 101 109 113 121 127			193 197 199 203 205 211 215 227 229 239 247 251
	131 137 143 151 157 169			259 265 269 275 281 289 295 307 311 317 319 329
	173 179 181 191 193 197			331 335 343 361 367 373 401 403 407 409 419 421
	205 223 229 235 263 265			425 427 455 461 467 485 493 497 499 509 511 517
	269 271			521 533 539 547
556	1 3 5 9 13 15	139	278	1 5 7 9 11 13 25 29 31 35 37 41
	19 23 25 27 29 37			45 47 49 51 55 57 63 65 67 69 71 77
	39 41 43 45 49 57			79 81 83 89 91 99 107 113 117 121 125 127
	59 65 69 75 77 81			129 131 137 143 145 155 159 163 167 169 173 175
	87 89 95 103 111 113			177 181 183 185 191 193 203 205 217 219 225 235
	115 117 119 121 123 125			239 245 251 255 257 259 261 263 275
	129 135 137 145 147 151			
	169 171 173 177 179 181			
	185 187 193 195 199 205			
	207 211 215 217 223 225			
	227 231 243 245 247 257			
	261 267 271			
		$140 = 35a^2$		
282	1 5 7 11 23 25	141	564	1 5 19 25 29 31 37 41 43 49 59 61
	29 35 37 41 49 55			67 71 77 83 91 95 97 113 119 121 125 127
	61 77 79 97 103 107			131 137 139 143 145 151 155 157 161 163 169 185
	113 115 121 125 137			187 191 199 205 211 215 221 223 233 239 241 245
				251 253 257 263 277 281 289 293 295 299 305 317
		(suite p. 176)		335 337 347 355 361 367 371 383 385 389 391 397

$\left(\frac{D}{x}\right)=1$. z^2-Dy^2. MODULE.	x.	D.	z^2+Dy^2, $\left(\frac{-D}{x}\right)=1$. MODULE.	x.
		141 (suite)	564	+413 431 449 455 457 461 463 475 479 485 491 499
				509 511 529 541 547 551 553 557
568	± 1 3 7 9 13 19	142	568	1 9 11 13 15 21 25 35 49 51 53 57
	21 23 25 27 31 39			59 61 67 69 73 79 81 85 87 89 93 95
	43 47 49 53 55 57			99 103 111 115 117 119 121 123 129 133 135 139
	61 63 69 73 75 81			141 143 145 149 151 155 161 163 165 167 169 173
	83 85 89 91 93 107			181 185 189 191 195 197 199 203 205 211 215 217
	117 121 127 129 131 133			223 225 227 231 233 235 249 259 263 269 271 273
	141 145 147 149 159 161			275 283 287 289 291 301 303 307 311 313 315 317
	165 169 171 173 175 179			321 323 325 327 329 331 339 347 349 359 361 367
	181 183 185 187 189 197			375 381 385 389 391 393 397 409 411 415 421 431
	205 207 217 219 225 233			437 441 443 455 459 461 463 467 471 477 485 491
	239 243 247 249 251 255			493 503 505 513 521 523 525 527 529 531 535 537
	267 269 273 279			539 541 545 549 551 561 563 565
572	1 9 15 21 25 31	143	286	1 3 7 9 19 21 23 25 27 41 49 53
	35 41 43 47 49 51			57 63 69 73 75 81 83 85 103 109 113 123
	53 57 59 67 69 71			133 145 147 149 151 155 157 159 161 167 171 175
	73 79 81 85 87 95			179 181 185 189 191 193 197 199 207 215 219 225
	107 109 111 113 115 119			227 235 239 241 243 249 251 255 257 269 271 281
	127 131 133 135 139 145			
	149 157 161 163 181 183			
	185 189 193 197 203 211			
	223 225 241 249 257 259			
	263 267 269 279 281 283			
		$144=a^2$		
290	1 3 9 17 27 37	145	580	1 7 9 11 17 19 23 31 37 39 49 63
	43 47 49 51 59 71			67 73 77 79 81 83 97 99 103 107 109 113
	73 77 81 91 97 109			119 121 123 129 131 133 137 141 149 153 157 159
	111 113 121 127 129 133			161 167 169 171 177 181 183 187 191 193 207 209
	137 139 141 143			211 213 217 223 227 241 251 253 259 267 271 273
				279 281 283 289 293 303 311 317 323 331 333 337
				341 343 347 349 351 359 361 379 381 383 391 401
				407 417 429 433 437 441 453 463 469 479 487 489
				491 509 511 519 521 523 527 529 533 537 539 547
				553 559 567 577
584	1 5 9 11 13 21	146	584	1 3 5 7 9 13 15 19 21 25 27 29
	23 25 29 41 43 45			31 35 39 41 45 47 49 53 57 63 65 67
	49 51 53 55 57 59			75 77 81 87 89 91 93 95 97 101 103 105
	65 71 77 79 81 83			117 121 123 125 133 135 137 141 145 147 151 155
	89 93 97 99 101 105			157 159 167 169 171 175 187 189 191 195 197 199
	107 111 115 117 121 125			201 203 205 211 217 225 227 229 235 239 243 245
	127 131 133 137 139 141	(suite p. 177)		247 251 253 257 261 263 265 267 271 273 277 279

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$.		D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$.	
MODULE.	x.		MODULE.	x.
584	±143 145 157 163 169 179	146	584	+283' 285 287 289 291 309 315 325 329 335 343 347
	183 189 197 201 205 207	(suite)		351 353 361 363 369 371 375 377 391 399 401 403
	215 217 223 225 229 231			405 407 411 419 421 423 431 435 441 445 453 455
	245 253 255 257 259 261			457 465 469 471 473 475 477 485 499 501 505 507
	265 273 275 277 285 289			513 515 523 525 529 533 541 547 551 561 567 573
		$147 = 3a^2$		
		$148 = 37a^2$		
298	1 5 7 9 17 19	149	596	1 3 5 9 11 15 17 23 25 27 29 33
	25 29 31 33 35 37			37 43 45 49 51 53 55 59 61 69 71 73
	39 45 47 49 53 61			75 79 81 83 85 87 91 99 111 113 115 121
	63 67 69 73 81 85			125 129 131 133 135 139 145 147 151 153 159 163
	95 103 107 113 119 121			165 167 169 173 177 183 185 187 199 207 211 213
	123 125 127 129 133 143			215 217 219 223 225 227 229 237 239 243 245 247
	145			249 253 255 261 265 269 271 273 275 281 283 287
				289 293 295 297 305 311 317 319 329 333 337 339
				345 355 361 363 367 375 387 391 393 395 399 401
				403 405 407 415 417 421 425 435 439 441 453 455
				459 469 473 477 479 487 489 491 493 495 499 501
				503 507 519 529 531 533 539 549 555 557 561 565
				575 577 583 589
		$150 = 6a^2$		
604	1 3 5 7 9 15	151	302	1 5 9 11 17 19 21 25 29 31 37 39
	17 21 23 25 27 29			43 45 47 49 55 59 69 81 85 91 95 97
	35 37 45 49 51 63			99 103 105 121 123 125 127 137 139 145 153 155
	67 69 71 75 79 81			159 161 167 169 171 173 183 185 187 189 191 193
	83 85 87 97 105 107			195 201 209 213 215 219 223 225 227 229 231 235
	111 115 119 121 125 131			237 239 241 245 249 251 261 267 269 275 279 287
	135 137 143 145 147 153			289 295 299
	161 163 169 173 175 179			
	185 183 193 199 201 203			
	207 209 211 213 225 229			
	237 241 243 245 247 249			
	255 259 261 263 269 271			
	283 289 291			
		$152 = 38a^2$		
		$153 = 17a^2$		
616	1 3 5 9 15 17	154	616	1 5 9 17 19 25 29 31 39 41 45 47
	23 25 27 29 41 43			67 69 73 79 81 83 85 95 103 109 111 113
	45 51 59 69 71 73			125 127 129 131 137 139 145 149 151 153 155 157
	75 81 85 87 107 109			159 163 169 171 177 179 181 183 195 197 199 205
	113 115 123 125 129 135			213 223 225 227 229 235 239 241 261 263 267 269
	137 145 149 153 157 167	(suite p. 178)		277 279 283 289 291 299 303 307 311 321 323 331

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
616	±169 177 181 191 197 205	154	616	335 345 351 359 361 365 367 369 373 379 383 395
	207 211 213 215 219 225	(suite)		397 401 405 409 415 423 425 431 443 449 475 481
	229 241 243 247 251 255			493 499 501 509 515 519 523 527 529 541 545 551
	261 269 271 277 289 295			555 557 559 563 565 573 579 589 593 601 603 613
620	1 7 9 11 13 17	155	310	1 3 9 13 17 19 23 27 37 39 41 43
	37 41 47 49 53 57			49 51 53 57 59 69 71 73 77 81 83 101
	63 67 69 73 77 79			109 111 117 121 123 127 129 131 137 147 149 153
	81 87 91 99 101 103			159 167 169 171 177 191 197 203 207 211 213 219
	107 109 117 119 121 129			221 223 231 243 247 249 263 277 281 289 299 303
	137 139 143 149 151 153			
	163 169 177 179 183 187			
	197 199 213 221 227 239			
	249 251 259 267 271 277			
	281 283 287 289 291 307			
		$156 = 39a^2$		
314	1 3 9 11 13 17	157	628	1 7 9 13 15 17 23 25 33 37 43 49
	19 25 27 31 33 35			55 57 59 63 79 81 83 87 89 91 93 95
	37 39 47 49 51 57			101 103 105 107 109 113 117 119 121 123 131 135
	67 71 75 81 89 93			139 141 145 151 153 155 159 161 163 169 173 175
	99 101 105 107 111 113			179 183 191 193 195 197 201 205 207 209 211 213
	115 117 121 127 141 143			219 221 223 225 227 231 233 235 251 255 257 259
	145 147 153			265 271 277 281 289 291 297 299 301 305 307 313
				317 319 325 333 335 341 343 345 349 353 355 359
				361 365 367 375 379 381 383 385 387 389 391 399
				411 413 425 429 439 441 443 447 451 457 461 463
				471 479 481 485 491 495 499 501 503 513 517 531
				543 551 553 555 557 559 561 563 567 575 577 581
				583 587 589 593 597 599 601 607 609 617 623 625
632	1 7 9 11 15 19	158	632	1 3 9 23 25 27 29 31 35 37 43 49
	25 29 37 39 47 49			53 55 59 61 65 69 73 75 77 81 85 87
	51 53 61 63 65 67			89 91 93 95 97 105 107 109 111 119 121 129
	69 71 73 77 81 83			133 139 143 147 149 151 157 159 165 167 169 173
	85 89 93 97 99 103			177 183 187 195 197 205 207 209 211 219 221 223
	105 109 115 121 123 127			225 227 229 231 235 239 241 243 247 251 255 257
	129 131 133 135 149 155			261 263 267 273 279 281 285 287 289 291 293 307
	157 163 165 169 171 173			313 315 321 323 327 329 331 333 335 337 349 355
	175 177 179 191 197 199			357 361 363 367 373 379 383 387 399 415 417 419
	203 205 209 215 221 225			429 431 433 439 441 443 447 451 453 457 461 469
	229 241 257 259 261 271			471 477 479 487 491 495 497 501 505 507 509 515
	273 275 281 283 285 289			517 519 529 531 533 549 561 565 569 575 581 585
	293 295 299 303 311 313			587 591 593 599 611 613 615 617 619 621 625 627
636	1 5 11 13 19 25	159 (suite p. 179)	318	1 5 7 13 23 25 35 37 41 43 49 65

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$.		D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$.	
MODULE.	x.		MODULE.	x.
636	± 31 37 41 47 49 55	159	318	+ 71 83 91 97 101 115 121 125 137 161 163 167
	59 65 67 79 95 97	(suite)		169 173 175 179 185 187 191 199 205 209 211 215
	101 103 107 119 121 125			223 229 233 239 241 245 251 257 259 263 271 287
	127 131 137 139 143 151			289 299 301 307
	155 161 169 173 185 203			
	205 209 227 229 233 235			
	241 245 247 257 275 283			
	289 295 301 311			
		$160 = 10a^2$		
322	1 5 9 17 19 25	161	644	1 3 5 9 11 15 17 25 27 29 31 33
	29 33 39 45 61 71			43 45 47 51 55 59 61 67 75 79 81 85
	81 83 85 89 93 95			87 89 93 97 99 107 121 125 129 131 135 139
	97 103 111 121 123 125			141 145 153 155 157 165 167 169 177 181 183 187
	127 129 141 143 145 151			191 193 197 201 215 223 225 229 233 235 237 241
	153 157 159			243 247 255 261 263 267 271 275 277 279 289 291
				293 295 297 305 307 311 313 317 319 321 335 341
				359 361 363 375 379 387 393 395 405 417 423 425
				431 433 435 439 445 449 459 465 471 473 481 485
				493 495 501 507 517 521 527 531 533 535 541 543
				549 561 571 573 579 587 591 603 605 607 625 631
		$162 = 2a^2$		
652	1 3 7 9 11 19	163	326	1 9 15 21 25 33 35 39 41 43 47 49
	21 23 25 27 31 33			51 53 55 57 61 65 69 71 77 81 83 85
	41 49 53 57 59 61			87 91 93 95 97 111 113 115 119 121 131 133
	63 65 67 69 75 77			135 143 145 151 155 161 167 169 173 177 179 185
	79 81 85 93 97 99			187 189 197 199 201 203 209 217 219 221 223 225
	103 107 113 121 123 127			227 237 247 251 253 259 263 267 281 289 295 297
	133 139 145 147 159 161			299 303 307 309 313 315 319 321 323
	169 171 173 175 177 183			
	185 189 191 195 197 201			
	207 209 211 215 217 221			
	225 231 235 237 239 243			
	253 255 271 275 279 281			
	283 287 289 291 297 309			
	311 313 321			
		$164 = 41a^2$		
330	1 7 13 23 29 31	165	660	1 13 19 29 41 49 53 59 67 71 73 79
	41 43 47 49 53 73			83 101 103 107 113 119 137 139 149 151 161 163
	91 101 112 127 131 137			167 169 179 181 191 193 211 217 223 227 229 247
	149 161			251 257 259 263 271 277 281 289 301 311 317 329
				337 347 353 361 367 373 377 391 419 421 427 439
		(suite p. 180)		457 461 463 487 503 527 529 533 551 563 569 571

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$.		D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$.	
MODULE.	x.		MODULE.	x.
330		165 (suite)	660	+599 613 617 623 629 637 643 653
664	± 1 3 5 9 11 13	166	664	1 5 7 9 13 17 19 23 25 31 33 35
	15 17 25 27 33 39			41 43 45 49 53 63 65 67 81 85 87 91
	41 45 47 49 51 53			95 101 107 111 113 115 117 119 121 125 127 133
	55 59 65 71 75 79			139 141 149 151 153 155 157 161 163 165 167 169
	81 85 99 101 103 113			171 175 177 179 181 183 191 193 199 205 207 211
	117 121 123 125 131 133			213 215 217 219 221 225 231 237 241 245 247 251
	135 141 143 147 149 153			265 267 269 279 283 287 289 291 297 299 301 307
	157 159 161 165 169 177			309 313 315 319 323 325 327 331 335 343 347 353
	181 187 193 195 203 205			359 361 369 371 379 383 387 389 391 393 401 403
	213 217 221 223 225 227			405 407 409 411 421 425 429 431 435 437 441 455
	235 237 239 241 243 245			461 463 467 469 473 475 479 491 505 517 519 521
	255 259 263 265 269 271			527 529 533 535 541 555 559 561 565 567 571 575
	275 289 295 297 301 303			585 587 589 591 593 595 603 605 607 609 613 617
	309 311 313 325			625 627 635 637 643 649 653 661
668	1 9 15 21 23 25	167	334	1 3 7 9 11 19 21 25 27 29 31 33
	29 33 35 39 43 49			47 49 57 61 63 65 75 77 81 85 87 89
	51 55 57 59 61 65			93 97 99 107 115 121 127 133 137 141 147 157
	67 71 77 79 81 83			169 171 173 175 179 181 183 185 189 191 195 199
	85 89 91 93 95 97			203 205 209 211 215 217 221 223 225 229 231 233
	103 111 119 121 123 131			239 243 251 255 261 263 265 267 275 279 281 283
	133 135 137 139 141 143			289 291 293 295 297 299 311 317 319 321 329
	151 155 157 159 163 169			
	173 181 185 187 189 205			
	207 209 217 219 221 225			
	227 229 233 235 247 259			
	261 265 271 281 287 289			
	293 297 303 307 315 317			
	321 323 327 329 331			
		$168 = 42\,a^2$		
		$169 = \quad a^2$		
680	1 7 9 11 13 23	170	680	1 3 9 13 19 27 29 31 39 47 49 53
	29 43 49 53 57 61			57 59 61 71 73 77 79 81 87 89 93 97
	63 67 73 77 81 83			103 107 109 113 117 121 127 141 147 157 159 161
	89 91 93 97 99 109			163 169 171 177 179 181 183 193 199 213 219 223
	111 113 117 121 123 131			227 231 233 237 243 247 251 253 259 261 263 267
	139 141 143 151 157 161			269 279 281 283 287 291 293 301 309 311 313 321
	167 169 177 181 191 193			327 331 337 339 347 351 361 363 373 377 381 383
	203 207 211 213 233 237			403 407 409 423 431 439 441 451 463 469 471 473
	239 253 261 269 271 281			477 479 483 489 491 507 513 529 531 537 541 543
	293 299 301 303 307 309			547 549 551 557 569 579 581 589 597 611 613 617
	313 319 321 337			637 639 643 647 657 659 669 673

$\left(\frac{D}{x}\right)=1$, z^2-Dy^2. MODULE.	x.	D.	z^2+Dy^2, $\left(\frac{-D}{x}\right)=1$. MODULE.	x.
		$171=19a^2$		
		$172=43a^2$		
346	± 1 9 13 15 21 23	173	692	+ 1 3 7 9 11 13 19 21 25 27 29 33
	25 29 31 33 35 37			37 39 41 49 57 59 63 71 73 75 77 79
	41 43 47 49 51 55			81 85 87 89 91 99 103 107 109 111 113 115
	57 67 73 77 81 83			117 121 123 127 131 133 137 143 147 149 155 157
	85 89 95 109 113 117			169 171 175 177 189 191 197 199 203 209 213 215
	119 121 133 135 137 139			219 223 225 229 231 233 235 237 239 243 247 255
	149 151 157 159 163 167			257 259 261 265 267 269 271 273 275 283 287 289
	169			297 305 307 313 317 319 321 325 327 333 335 337
				339 343 345 351 361 363 369 377 381 389 391 393
				397 399 401 407 411 413 415 429 439 441 443 447
				451 465 471 475 481 485 487 491 497 499 505 507
				509 511 513 525 527 529 531 533 539 541 547 551
				553 557 563 567 573 587 591 595 597 599 609 623
				625 627 631 637 639 641 645 647 649 655 657 661
				669 675 677 687
696	1 5 11 17 23 25	174	696	1 5 7 17 19 25 35 37 41 43 47 49
	31 37 41 49 53 55			53 59 61 83 85 89 95 103 107 113 119 121
	67 71 79 85 89 91			125 133 137 143 149 151 157 163 169 173 175 179
	113 115 121 125 127 131			185 191 197 199 205 211 215 223 227 229 235 241
	133 137 139 149 155 157			245 253 259 263 265 287 289 295 299 301 305 307
	167 169 173 185 187 197			311 313 323 329 331 341 343 347 359 361 371 379
	203 205 229 239 241 245			403 413 415 419 421 425 427 439 445 449 457 463
	247 251 253 265 271 275			475 479 487 503 509 515 529 535 541 557 565 569
	283 289 301 305 313 329			581 587 595 599 605 617 619 623 625 629 631 641
	335 341			665 673 683 685
		$175=7a^2$		
		$176=11a^2$		
354	1 7 11 19 23 25	177	708	1 25 31 35 43 49 55 65 67 71 77 85
	47 49 65 77 79 83			89 91 95 101 103 107 113 115 119 121 133 143
	85 89 101 113 121 127			145 149 151 161 167 169 173 181 185 187 193 203
	131 133 139 145 149 155			205 209 211 221 233 235 239 241 247 251 253 259
	161 163 169 173 175			263 265 269 277 283 287 289 299 305 311 319 323
				329 353 359 361 365 367 371 373 377 383 391 395
				401 407 415 427 433 437 451 463 479 481 485 491
				493 509 511 517 529 533 545 551 553 569 571 577
				581 583 599 611 625 629 635 647 655 661 667 671
				679 685 689 691 695 697 701 703
712	1 3 9 13 17 19	178	712	1 7 9 11 13 15 17 23 25 29 31 37
	25 27 29 35 37 39			49 57 61 63 67 73 77 81 91 95 97 99
	43 47 49 51 55 57	(suite p. 182)		101 103 105 107 117 119 121 123 127 129 131 135

$\left(\frac{D}{x}\right)=1$, z^2-Dy^2.		D.	z^2+Dy^2, $\left(\frac{-D}{x}\right)=1$.	
MODULE.	x.		MODULE.	x.
712	± 59 61 71 73 75 77	178 (suite)	712	+ 139 141 143 149 151 153 159 161 165 169 175 177
	79 81 83 87 97 101			179 181 187 191 195 197 203 205 207 213 215 217
	105 111 115 117 121 129			221 225 227 229 233 235 237 239 249 251 253 255
	141 147 149 153 155 161			257 259 261 265 275 279 283 289 293 295 299 307
	163 165 167 169 171 177			319 325 327 331 333 339 341 343 345 347 349 355
	181 183 197 199 205 211			359 361 375 377 383 389 391 395 397 399 401 403
	213 217 219 221 223 225			407 409 411 415 421 425 427 431 435 439 441 443
	229 231 233 237 243 247			449 465 467 469 471 481 489 493 501 503 511 513
	249 253 257 261 263 265			519 523 527 529 539 541 545 549 555 557 565 567
	271 287 289 291 293 303			575 579 587 597 599 601 603 619 625 627 629 633
	311 315 323 325 333 335			637 641 643 647 653 657 659 661 665 667 669 671
	341 345 349 351			673 677 679 685 691 693 707 709
716	1 5 7 9 11 13	179	358	1 3 5 9 13 15 17 19 25 27 29 31
	17 23 25 29 35 45			39 43 45 47 49 51 57 59 61 65 67 75
	49 55 57 61 63 65			77 81 83 85 87 89 93 95 101 107 117 121
	71 77 79 81 85 89			125 129 135 139 141 145 147 149 151 153 155 161
	91 93 99 101 103 111			169 171 173 177 183 191 193 195 199 201 215 221
	115 117 119 121 123 125			225 227 231 235 239 243 245 247 249 253 255 259
	127 129 131 141 143 145			261 267 279 285 287 289 295 303 305 317 321 323
	149 153 159 161 163 167			325 335 337 347 351
	169 173 175 177 187 193			
	201 203 207 211 219 221			
	223 225 245 249 251 253			
	261 263 271 275 283 285			
	289 291 299 305 307 311			
	315 317 319 321 325 327			
	331 337 339 343 355			
		$180=5a^2$		
362	1 3 5 9 11 13	181	724	1 5 7 9 13 19 23 25 29 31 33 35
	15 25 27 29 33 37			37 45 47 49 51 63 65 71 73 81 83 91
	39 43 45 49 55 59			95 101 103 107 115 117 121 123 125 127 129 131
	65 67 73 75 79 81			133 137 145 151 155 159 161 163 165 169 171 175
	87 99 101 111 117 119			177 179 183 185 187 191 193 197 199 201 203 207
	121 125 129 133 135 137			211 217 225 229 231 233 235 237 239 241 245 247
	139 143 145 147 161 165			255 259 261 267 271 279 281 289 291 297 299 311
	167 169 177			313 315 317 325 327 329 331 333 337 339 343 349
				353 355 359 361 365 373 377 379 383 389 401 403
				405 415 417 419 421 423 429 431 437 439 441 447
				449 451 455 459 491 467 471 473 475 481 497 501
				503 505 509 511 515 519 529 535 551 557 567 571
				575 577 581 583 585 589 605 611 613 615 619 625
		(suite p. 183)		627 631 635 637 639 645 647 649 655 657 663 665

$\left(\frac{D}{x}\right) = 1$, $z^2 - Dy^2$. MODULE.	x.	D.	$z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
362		181 (suite)	724	+667 669 671 681 683 685 697 703 707 709 713 719
728	± 1 3 5 9 11 15	182	728	1 5 9 19 23 25 29 31 33 41 43 45
	25 27 29 33 41 45			47 51 53 59 73 79 81 83 89 95 97 107
	53 55 67 71 73 75			111 113 115 121 125 127 145 155 165 167 171 179
	81 87 89 97 99 103			183 187 191 201 205 207 211 213 215 223 225 227
	113 121 123 125 131 135			229 233 235 241 255 261 263 265 271 277 279 289
	139 145 151 159 163 165			293 295 297 303 307 309 327 337 347 349 353 361
	199 201 205 213 219 225			365 369 373 383 387 389 393 395 397 405 407 409
	229 233 239 241 243 251			411 415 417 423 437 443 445 447 453 459 461 471
	261 265 267 275 277 283			475 477 479 485 489 491 509 519 529 531 535 543
	289 291 293 297 309 311			547 551 555 565 569 571 575 577 579 587 589 591
	319 323 331 335 337 339			593 597 599 605 619 625 627 629 635 641 643 653
	349 353 355 359 361 363			657 659 661 667 671 673 691 701 711 713 717 725
732	1 7 13 17 25 29	183	366	1 11 13 17 19 23 25 29 35 49 53 59
	31 43 47 49 53 55			71 73 89 97 101 103 109 121 127 143 155 163
	67 73 79 83 89 91			169 173 185 187 191 199 205 209 215 217 221 227
	95 97 101 107 109 115			229 233 235 241 247 251 253 259 271 275 281 283
	119 121 131 139 151 167			287 289 299 301 311 319 323 325 329 335 359 361
	169 173 175 179 185 203			
	205 209 211 217 221 223			
	229 233 239 241 253 263			
	281 289 295 301 307 325			
	329 331 343 347 355 361			
		$184 = 46a^2$		
370	1 9 11 13 17 21	185	740	1 3 7 9 13 17 19 21 27 31 39 41
	23 41 43 49 57 71			47 49 51 57 59 63 67 79 81 83 91 93
	81 87 93 97 99 101			97 101 107 113 117 119 121 123 127 131 133 141
	103 113 117 121 133 139			147 149 153 169 171 177 179 181 189 191 193 199
	141 143 149 151 153 159			201 217 221 223 229 237 239 243 247 249 251 257
	163 167 169 177 181 183			263 269 273 277 279 287 289 291 303 307 311 313
				319 321 323 329 331 339 343 349 351 353 357 361
				363 367 369 381 393 399 403 413 423 431 439 441
				443 447 457 459 469 473 479 499 507 509 513 521
				527 529 531 533 537 543 553 557 567 573 577 579
				581 583 589 597 601 603 611 631 637 641 651 653
				661 663 667 669 671 679 687 697 707 711 717 729
744	1 5 7 13 17 23	186	744	1 5 11 13 17 19 25 37 47 49 55 61
	25 35 37 43 49 59			65 67 71 79 83 85 89 95 97 101 121 125
	61 65 85 89 91 97			127 137 143 149 151 161 163 169 173 179 181 185
	101 103 107 115 119 121			187 191 193 199 203 209 211 221 223 229 235 245
	125 131 137 139 149 161			247 251 271 275 277 283 287 289 293 301 305 307
	167 169 173 175 181 185	(suite p. 184)		311 317 323 325 335 347 353 355 359 361 367 371

$\left(\frac{D}{x}\right) = 1$, $Z^2 - Dy^2$.		D.	$Z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$.	
MODULE.	x.		MODULE.	x.
744	±193 209 215 221 227 229	186	744	+379 395 401 407 413 415 425 431 445 449 463 475
	239 245 259 263 277 289			479 481 485 487 491 503 505 511 517 529 539 547
	293 295 299 301 305 317			569 577 587 599 605 611 613 625 629 631 635 637
	319 325 331 343 353 361			641 653 667 671 685 691 701 703 709 715 721 737
748	1 3 9 19 23 25	187	374	1 7 9 15 25 29 39 41 47 49 53 57
	27 29 31 35 41 43			59 61 63 65 67 69 73 79 81 89 93 95
	49 53 57 61 65 69			103 105 107 109 111 115 129 131 135 137 139 155
	71 73 75 81 83 87			157 167 169 173 175 179 185 191 193 197 203 211
	89 91 93 105 109 123			213 215 223 225 227 229 233 241 247 249 251 257
	127 129 137 147 151 157			261 273 277 283 287 291 299 303 329 331 337 339
	159 163 169 171 173 183			343 347 351 353 355 361 369 371
	185 193 195 197 199 207			
	213 219 225 229 233 235			
	239 241 243 249 257 259			
	261 263 267 271 273 277			
	279 295 307 311 315 327			
	329 335 337 353 359 361			
	367 369			
		$188 = 47a^2$		
		$189 = 21a^2$		
760	1 3 7 9 11 21	190	760	1 9 21 29 33 39 43 49 51 59 69 77
	23 27 29 31 33 47			81 83 91 93 97 103 109 111 113 119 121 123
	49 63 67 69 71 77			127 141 143 157 159 161 163 167 169 179 181 183
	79 81 87 93 97 99			187 189 191 193 197 199 201 211 213 217 219 221
	107 109 113 119 121 131			223 237 239 253 257 259 261 267 269 271 277 283
	139 141 147 151 157 161			287 289 297 299 303 311 321 329 331 337 341 347
	169 181 189 193 201 203			351 359 371 379 383 387 391 393 397 403 407 411
	207 213 217 221 227 231			417 421 427 433 441 443 447 451 453 459 467 469
	237 243 251 253 257 261			479 481 487 497 509 511 517 519 527 529 531 533
	263 269 277 279 289 291			553 557 583 587 607 609 611 613 621 623 629 631
	297 307 319 321 327 329			643 653 659 661 671 673 681 687 689 693 697 699
	337 339 341 343 363 367			707 713 719 723 729 733 737 743 747 749 753 757
764	1 5 7 9 11 13	191	382	1 3 5 9 13 15 17 23 25 27 39 43
	17 19 25 31 35 45			45 49 51 59 65 67 69 75 77 79 81 85
	47 49 55 63 65 69			97 103 107 109 115 117 121 125 129 133 135 147
	71 77 81 83 85 87			149 153 163 169 177 193 195 197 199 201 203 207
	91 95 97 99 109 111			209 211 215 217 221 223 225 227 231 237 239 241
	117 119 121 123 125 127			243 245 251 255 259 263 269 271 277 281 283 287
	129 131 133 139 143 149			289 291 293 295 299 309 311 319 321 325 327 329
	151 153 155 159 167 169			335 341 345 347 349 351 353 361 363 371 375
	171 173 177 179 183 187			
	193 197 201 209 217 219			

$\left(\frac{D}{x}\right) = 1$, $Z^2 - Dy^2$. MODULE.	x.	D.	$Z^2 + Dy^2$, $\left(\frac{-D}{x}\right) = 1$. MODULE.	x.
764	±221 225 235 237 241 245	191	382	
	247 267 269 271 277 279			
	281 289 293 303 307 309			
	315 321 323 325 329 331			
	339 341 343 345 349 353			
	355 359 361 367 379			
		$192 = 3a^2$		
386	1 3 7 9 21 23	193	772	+ 1 9 11 15 19 21 25 35 39 47 49 51
	25 27 31 43 49 55			65 69 71 79 81 85 87 91 93 97 99 101
	59 63 65 67 69 75			103 109 111 115 119 121 123 127 129 135 137 145
	81 83 85 93 95 97			157 159 161 163 165 167 169 171 177 181 183 185
	101 107 109 121 131 137			189 197 201 203 205 209 215 217 219 221 223 225
	139 143 145 147 151 155			227 229 241 249 251 257 259 263 265 267 271 275
	157 161 165 169 175 177			277 283 285 287 289 293 295 299 301 305 307 315
	179 181 185 187 189 191			317 321 335 337 339 347 351 361 365 367 371 375
				377 385 389 391 393 399 403 409 413 415 417 419
				423 427 429 431 439 441 443 445 447 449 453 459
				461 463 469 475 481 491 493 499 503 511 517 519
				525 527 529 533 535 537 539 541 559 561 565 573
				577 581 585 593 597 599 617 619 621 623 625 629
				631 633 639 641 647 655 659 665 667 677 683 689
				695 697 699 705 709 711 713 715 717 719 727 729
				731 735 739 741 743 745 749 755 759 765 767 769
776	1 5 9 13 19 21	194	776	1 3 5 7 9 11 13 15 21 23 25 27
	25 29 31 33 37 45			29 33 35 37 39 43 45 49 55 63 65 69
	41 49 51 59 65 67			71 73 75 77 81 87 89 91 99 105 111 113
	69 73 77 79 81 83			115 117 121 125 127 129 135 143 145 147 149 157
	89 95 103 105 107 113			161 163 165 169 173 175 181 185 189 193 195 199
	117 119 121 123 125 129			203 207 213 215 219 223 225 227 231 239 241 243
	131 139 145 149 151 155			245 253 259 261 263 267 271 273 275 277 283 289
	157 159 161 165 167 169			297 299 301 307 311 313 315 317 319 323 325 333
	171 173 179 181 183 185			339 343 345 349 351 353 355 359 361 363 365 367
	187 189 191 193 211 213			373 375 377 379 381 383 385 387 405 407 419 429
	225 235 241 245 247 251			435 439 441 445 447 449 453 467 471 473 481 483
	253 255 261 273 277 279			489 491 495 497 507 511 519 521 525 527 529 539
	287 289 295 297 301 303			541 543 547 555 559 565 567 571 575 579 585 589
	313 317 325 327 331 333			593 597 599 605 609 617 621 623 625 635 637 639
	335 345 347 349 353 361			643 645 653 657 667 669 673 675 681 683 691 693
	365 371 373 377 381 385			697 709 715 717 719 723 725 729 735 745 757 759
780	1 17 19 31 37 41	195	390	1 7 11 17 23 37 41 49 53 59 61 67
	43 47 49 53 61 73			71 73 77 79 89 97 107 113 119 121 139 149
	77 83 89 97 103 113			161 163 173 181 187 193 199 211 223 233 239 253

$\left(\frac{D}{x}\right) = 1$, $Z^2 - Dy^2$.							D.	$Z^2 = Dy^2$, $\left(\frac{-D}{x}\right) = 1$.												
MODULE.	x.							MODULE.	x.											
780	±121	127	131	149	151	161	195	390	+257	259	263	281	287	289	307	343	347	359	361	371
	167	173	179	181	191	193														
	203	227	233	251	253	257														
	271	281	283	289	311	319														
	323	331	361	367	379	383														
							$196 = a^2$													
394	1	7	9	15	19	23	197	788	1	3	9	11	25	27	29	31	33	35	37	41
	25	29	33	37	39	41			49	53	61	65	67	71	75	79	81	85	87	91
	43	47	49	51	53	55			93	95	97	99	101	103	105	109	111	115	119	121
	59	61	63	65	81	83			123	131	133	137	139	147	151	157	159	161	167	169
	85	93	97	101	105	107			173	179	181	183	193	195	191	201	211	213	215	221
	109	121	127	133	135	137			225	227	233	235	237	243	247	255	257	261	263	271
	143	155	157	161	163	169			273	275	279	283	285	289	291	293	295	297	299	301
	171	173	175	181	187	191			303	307	309	313	315	319	323	327	329	333	341	345
	193								353	357	359	361	363	365	367	369	383	385	391	393
									399	401	407	409	411	413	415	417	433	437	439	441
									445	449	451	453	457	463	467	471	477	483	501	507
									511	519	521	523	529	535	537	539	543	547	549	557
									559	565	569	571	579	581	583	585	597	599	601	603
									611	613	617	623	625	633	635	639	643	645	647	653
									659	661	663	671	675	681	699	705	711	715	719	725
									729	731	733	737	741	743	745	749	765	767	769	771
									773	775	781	783								
							$198 = 22a^2$													
796	1	3	5	9	11	13	199	398	1	5	7	9	13	23	25	29	31	33	35	43
	15	19	25	27	29	33			45	47	49	51	53	57	61	63	65	79	81	89
	39	45	49	53	55	57			91	103	111	115	117	121	123	125	131	139	145	151
	59	61	65	67	71	75			155	157	161	165	169	175	177	187	193	201	203	207
	81	83	87	89	95	99			209	213	215	217	219	225	227	231	235	239	245	249
	107	117	119	121	125	127			251	255	261	263	265	269	271	279	285	289	291	293
	135	143	145	147	157	159			297	299	301	303	305	309	311	313	315	321	323	325
	161	163	165	167	169	171			327	329	331	339	343	357	359	361	377	379	381	383
	177	179	183	191	193	195			387	395										
	201	209	211	213	217	223														
	225	243	245	247	249	259														
	261	265	267	269	275	283														
	285	287	289	293	295	297														
	301	305	307	309	313	319														
	321	325	329	335	347	351														
	355	357	361	363	367	375														
	377	381	391																	
							$200 = 2a^2$													

III. — **Valeurs** (mod. 2^n) **de** a, b, x **et** y **dans** $a^2+b^2=x^2-y^2=\text{N}$.

N.	a ou b.	x.	
$4k+$	$2a\pm$	$2a\pm$	$4k+$
1	1	1	3
3	–	0	1
$16k+$	$8a\pm$	$8a\pm$	$16k+$
1	1	1	15
3	–	2	13
5	1	3	11
7	–	0, 4	9
9	3	3	7
11	–	2	5
13	3	1	3
15	–	0, 4	1
$32k+$	$16a\pm$	$16a\pm$	$32k+$
5	1	3	27
13	3	7	19
21	7	5	11
29	5	1	3
$64k+$	$32a\pm$	$32a\pm$	$64k+$
1	1, 7	1, 9	63
9	3, 11	3, 5	55
17	1, 9	9, 15	47
25	3, 5	5, 13	39
33	9, 15	7, 15	31
41	5, 13	11, 13	23
49	7, 15	1, 7	15
57	11, 13	3, 11	7
		y	N

N.	a ou b.		x.		
$256k+$	$64a\pm$	$128a\pm$	$64k\pm$	$128a\pm$	$256k+$
1	25	1, 31	23	1, 33	255
9	11	3, 35	5	3, 29	247
17	1	23, 55	17	9, 23	239
25	3	5, 27	13	5, 37	231
33	23	15, 17	7	17, 49	223
41	5	45, 51	21	19, 51	215
49	17	7, 39	31	7, 25	207
57	13	43, 53	29	11, 43	199
65	7	1, 33	9	33, 63	191
73	21	3, 29	27	29, 61	183
81	31	9, 23	15	9, 41	175
89	29	5, 37	19	37, 59	167
97	9	17, 49	25	47, 49	159
105	27	19, 51	11	13, 19	151
113	15	7, 25	1	25, 57	143
121	19	11, 43	3	11, 21	135
129	25	33, 63	23	31, 63	127
137	11	29, 61	5	35, 61	119
145	1	9, 41	17	41, 55	111
153	3	37, 59	13	27, 59	103
161	23	47, 49	7	15, 47	95
169	5	13, 19	21	13, 45	87
177	17	25, 57	31	39, 57	79
185	13	11, 21	29	21, 53	71
193	7	31, 63	9	1, 31	63
201	21	35, 61	27	3, 35	55
209	31	41, 55	15	23, 55	47
217	29	27, 59	19	5, 27	39
225	9	15, 47	25	15, 17	31
233	27	13, 45	11	45, 51	23
241	15	39, 57	1	7, 39	15
249	19	21, 53	3	43, 53	7
			y		N

III. — **Valeurs** (mod. 2^n) **de** a, b, x **et** y **dans** $a^2+b^2=x^2-y^2=\mathrm{N}$ (*suite*).

N.	*a* ou *b*.			*x*.			
$1024k+$	$64a\pm$	$256a\pm$	$512a\pm$	$64a\pm$	$256a\pm$	$512a\pm$	$1024k+$
1	25	31	1,127	23	33	1,129	1023
9	11	93	3,131	5	99	3,125	1015
17	1	55	105,233	17	9	151,233	1007
25	3	101	5,123	13	91	5,133	999
33	23	113	111,239	7	79	17,111	991
41	5	45	77,205	21	109	179,205	983
49	17	39	7,135	31	25	7,121	975
57	13	75	43,85	29	11	85,213	967
65	7	1	33,95	9	65	33,161	959
73	21	3	29,167	27	61	167,227	951
81	31	23	9,119	15	41	9,137	943
89	29	5	91,219	19	69	37,191	935
97	9	111	79,207	25	47	49,79	927
105	27	51	147,237	11	13	19,147	919
113	15	7	153,231	1	57	103,231	911
121	19	85	11,139	3	107	11,117	903
129	25	33	63,65	23	97	65,193	895
137	11	99	189,195	5	35	67,195	887
145	1	9	169,215	17	73	87,215	879
153	3	91	187,197	13	27	59,187	871
161	23	79	47,175	7	15	47,81	863
169	5	109	13,115	21	83	13,141	855
177	17	25	57,71	31	89	57,185	847
185	13	11	107,235	29	53	21,107	839
193	7	65	31,97	9	127	97,225	831
201	21	61	35,163	27	125	35,93	823
209	31	41	55,73	15	105	73,201	815
217	29	69	101,229	19	123	155,229	807
225	9	47	15,143	25	17	15,113	799
233	27	13	45,173	21	77	173,211	791
241	15	57	167,217	1	121	39,167	783
249	19	107	181,203	3	43	75,203	775
257	25	97	1,129	23	95	129,255	767
265	11	35	3,125	5	29	125,233	759
273	1	73	151,233	17	119	23,151	751
281	3	27	5,133	13	37	133,251	743
289	23	15	17,111	7	49	17,145	735
297	5	83	179,205	21	19	51,179	727
305	17	89	7,121	31	103	121,249	719
313	13	53	85,213	29	117	171,213	711
321	7	127	33,161	9	63	161,223	703
329	21	125	167,227	27	67	99,227	695
337	31	105	9,137	15	87	137,247	687
345	29	123	37,91	19	59	37,165	679
353	9	17	49,79	25	81	49,177	671
361	27	77	19,147	11	115	19,109	663
369	15	121	103,231	1	71	25,103	655
377	19	43	11,117	3	21	117,245	647
385	25	95	65,193	23	31	191,243	639
				y			N

N.	*a* ou *b*.			*x*.			
$1024k+$	$64a\pm$	$256a\pm$	$512a\pm$	$64a\pm$	$256a\pm$	$512a\pm$	$1024k+$
393	11	29	67,195	5	93	61,67	631
401	1	119	87,215	17	55	41,87	623
409	3	37	59,187	13	101	59,69	615
417	23	49	47,81	7	113	81,209	607
425	5	19	13,141	21	45	141,243	599
433	17	103	57,185	31	39	185,199	591
441	13	117	21,107	29	75	21,149	583
449	7	63	97,225	9	1	159,225	575
457	21	67	35,93	27	3	93,221	567
465	31	87	73,201	15	23	183,201	559
473	29	59	155,229	19	5	27,155	551
481	9	81	15,113	25	111	113,241	543
489	27	115	173,211	21	51	83,211	535
497	15	71	39,167	1	7	39,89	527
505	19	21	75,203	3	85	53,75	519
513	25	31	129,255	23	33	127,255	511
521	11	93	125,253	5	99	131,253	503
529	1	55	23,151	17	9	23,105	495
537	3	101	133,251	13	91	123,251	487
545	23	113	17,145	7	79	145,239	479
553	5	45	51,179	21	109	51,77	471
561	17	39	121,249	31	25	135,249	463
569	13	75	171,213	29	11	43,171	455
577	7	1	161,223	9	65	95,223	447
585	21	3	99,227	27	61	29,99	439
593	31	23	137,247	15	41	119,247	431
601	29	5	37,165	19	49	165,219	423
609	9	111	49,177	25	47	177,207	415
617	27	51	19,109	11	13	109,237	407
625	15	7	25,103	1	57	25,153	399
633	19	85	117,245	3	107	139,245	391
641	25	33	191,193	23	97	63,193	383
649	11	99	61,67	5	35	61,189	375
657	1	9	41,87	17	73	41,169	367
665	3	91	59,69	13	27	69,197	359
673	23	79	81,209	7	15	175,209	351
681	5	109	141,243	21	83	115,243	343
689	17	25	185,199	31	89	71,199	335
697	13	11	21,149	29	53	149,235	327
705	7	65	159,225	9	127	31,159	319
713	21	61	93,221	27	125	163,221	311
721	31	41	183,201	15	105	55,183	303
729	29	69	27,155	19	123	27,101	295
737	9	47	113,241	25	17	143,241	287
745	27	13	83,211	21	77	45,83	279
753	15	57	39,89	1	121	89,217	271
761	19	107	53,75	3	43	53,181	263
769	25	97	127,255	23	95	1,127	255
777	11	35	131,253	5	29	3,131	247
				y			N

III. — **Valeurs** (mod. 2^n) **de** a, b, x **et** y **dans** $a^2+b^2=x^2-y^2=\mathrm{N}$ (*suite*).

N. $1024k+$	*a* ou *b*. $64a\pm$	$256a\pm$	$512a\pm$	*x*. $64a\pm$	$256a\pm$	$512a\pm$	$1024k+$
785	1	73	23,105	17	119	105,233	239
793	3	27	123,251	13	37	5,123	231
801	23	15	145,239	7	49	111,239	223
809	5	83	51,77	21	19	77,205	215
817	17	89	135,249	31	103	7,135	207
825	13	53	43,171	29	117	43,85	199
833	7	127	95,223	9	63	33,95	191
841	21	125	29,99	27	67	29,167	183
849	31	105	119,247	15	87	9,119	175
857	29	123	165,219	19	59	91,219	167
865	9	17	177,207	25	81	79,207	159
873	27	77	109,237	11	115	147,237	151
881	15	121	25,153	1	71	153,231	143
889	19	43	139,245	3	21	11,139	135
897	25	95	63,193	23	31	63,65	127
				y			N

N. $1024k+$	*a* ou *b*. $64a\pm$	$256a\pm$	$512a\pm$	*x*. $64a\pm$	$256a\pm$	$512a\pm$	$1024k+$
905	11	29	61,189	5	93	189,195	119
913	1	119	41,169	17	55	169,215	111
921	3	37	69,197	13	101	187,197	103
929	23	49	175,209	7	113	47,175	95
937	5	19	115,243	21	45	13,115	87
945	17	103	71,199	31	39	57,71	79
953	13	117	149,235	29	75	107,235	71
961	7	63	31,159	9	1	31,97	63
969	21	67	163,221	27	3	35,163	55
977	31	87	55,183	15	23	55,73	47
985	29	59	27,101	19	5	101,229	39
993	9	81	143,241	25	111	15,143	31
1001	27	115	45,83	21	51	45,173	23
1009	15	71	89,217	1	7	167,217	15
1017	19	21	53,181	3	85	181,203	7
				y			N

N. $4096k+$	*a* ou *b*. $64a\pm$	$256a\pm$	$1024a\pm$	$2048a\pm$	*x*. $64a\pm$	$256a\pm$	$1024a\pm$	$2048a\pm$	$4096k+$
1	25	31	127	1,511	23	33	129	1,513	4095
257	25	97	1	129,383	23	95	257	129,641	3839
513	25	31	129	255,257	23	33	385	257,769	3583
769	25	97	257	127,385	23	95	511	385,897	3327
1025	25	31	385	1,513	23	33	383	513,1023	3071
1281	25	97	511	129,641	23	95	255	641,895	2815
1537	25	31	383	257,769	23	33	127	767,769	2559
1793	25	97	255	385,897	23	95	1	639,897	2303
2049	25	31	127	513,1023	23	33	129	511,1023	2047
2305	25	97	1	641,895	23	95	257	383,895	1791
2561	25	31	129	767,769	23	33	385	255,767	1535
2817	25	97	257	639,897	23	95	511	127,639	1279
3073	25	31	385	511,1023	23	33	383	1,511	1023
3329	25	97	511	383,895	23	95	255	129,383	767
3585	25	31	383	255,767	23	33	127	255,257	511
3841	25	97	255	127,639	23	95	1	127,385	255
					y				N

Si N est de la forme $8k+1$, a, b et x peuvent être limités à 2 cas sur 64, 2 sur 256, 2 sur 1024 etc., soit à la limite à 1 cas sur 24. Il en est de même de y pour $\mathrm{N}\equiv 7$ (mod. 8).

III. — Valeur (mod. ρ) de a, b, x, y, z, t

dans $a^2 + b^2 = x^2 - y^2 = z^2 + rn^2 + t^2 + nv^2 = \text{N}$.

r désigne un résidu quelconque et *n* un non-résidu (mod. ρ).

N.	$a, b, z.$			$x, t.$	
$3k+1$	$3k \pm 0$	1		–	2
2	1			0	$1 + 3k$
$9k+1$	$3k+0$	$9k \pm 1$		–	8
4	0	2		–	5
7	0	4		–	$2 + 9k$
$27k+1$	$3k+0$	$27k \pm 1.8$		–	26
4	0	2, 11		–	23
7	0	4, 13		–	20
10	0	8, 10		–	17
13	0	7, 11		–	14
16	0	4, 5		–	11
19	0	1, 10		–	8
22	0	2, 7		–	5
25	0	5, 13		–	$2 + 27k$
$81k+1$	$3k+0$	$27k \pm 8$,	$81k \pm 1$	–	80
4	0	11	2	–	77
7	0	4	13	–	74
10	0	10	35	–	71
13	0	7	16	–	68
16	0	5	4	–	65
19	0	1	10	–	62
22	0	2	34	–	59
25	0	13	5	–	56
28	0	8	26	–	53
31	0	11	29	–	50
34	0	4	14	–	47
37	0	10	19	–	44
40	0	7	11	–	41
43	0	5	23	–	38
46	0	1	17	–	35
49	0	2	7	–	32
52	0	13	32	–	29
55	0	8	28	–	26
58	0	11	25	–	23
61	0	4	40	–	20
64	0	10	8	–	17
67	0	7	38	–	14
70	0	5	31	–	11
73	0	1	37	–	8
76	0	2	20	–	5
79	0	13	22	–	$2 + 81k$
		y			N

III. — **Valeur** (mod. ρ) **de** a, b, x, y, z, t

dans $a^2 + b^2 = x^2 - y^2 = z^2 + rn^2 = t^2 + nv^2 = \mathrm{N}$ (*suite*).

r désigne un résidu quelconque et n un non-résidu (mod. ρ).

N.	$a, b, x, z.$		$t.$	
$5k +$ 1	$5k \pm 0$	1	2	4
2	1		0, 2	3
3	2		0, 1	2
4	0	2	1	$1 + 5k$
$25k +$ 1	$5k + 0$	$25k \pm$ 1	$5k + 2$	24
4	0	2	1	21
6	0	9	2	19
9	0	3	1	16
11	0	6	2	14
14	0	8	1	11
16	0	4	2	9
19	0	12	1	6
21	0	11	2	4
24	0	7	1	$1 + 25k$
$125k +$ 1	$5k + 0$	$125k \pm$ 1 49 51	2	124
4	0	2 23 27	1	111
6	0	16 34 59	2	119
9	0	3 22 28	1	116
11	0	6 19 56	2	114
14	0	17 42 58	1	111
16	0	4 46 54	2	109
19	0	12 13 37	1	106
21	0	11 36 39	2	104
24	0	7 32 57	1	101
26	0	1 26 49	2	99
29	0	2 23 48	1	96
31	0	16 34 41	2	94
34	0	3 28 53	1	91
36	0	6 44 56	2	89
39	0	8 17 42	1	86
41	0	4 21 54	2	84
44	0	12 13 38	1	81
46	0	14 36 39	2	79
49	0	7 18 32	1	76
51	0	24 26 49	2	74
54	0	23 48 52	1	71
56	0	9 34 41	2	69
59	0	28 47 53	1	66
61	0	6 31 44	2	64
64	0	8 17 33	1	61
66	0	21 29 54	2	59
69	0	13 38 62	1	56
71	0	14 36 61	2	54
74	0	7 18 43	1	51
76	0	24 26 51	2	49
79	0	27 48 52	1	46
81	0	9 41 59	2	44
84	0	22 47 53	1	41
		y		N

III. — **Valeur** (mod. ρ) **de** a, b, x, y, z,

dans $a^2+b^2=x^2-y^2=z^2+rn^2=t^2+nv^2=$ N (*suite*).

r désigne un résidu quelconque et n un non-résidu (mod. ρ).

N.	$a, b, x, z.$		$t.$	
$125k+86$	$5k+0$	$125k\pm19$ 31 44	2	39
89	0	8 33 58	1	36
91	0	21 29 46	2	34
94	0	37 38 62	1	31
96	0	11 14 61	2	29
99	0	18 43 57	1	26
101	0	1 24 51	2	24
104	0	2 27 52	1	21
106	0	9 16 59	2	19
109	0	3 22 47	1	16
111	0	19 31 56	2	14
114	0	33 42 58	1	11
116	0	4 29 46	2	9
119	0	12 37 62	1	6
121	0	11 39 61	2	4
124	0	32 43 57	1	$1+125k$
		y		N

N.	$a, b, z.$		$x, t.$	
$7k+$ 1	$7k\pm0$ 2	1	3	6
2	0 1	3	2	5
3	1 3		0 2	4
4	0 3	2	1	3
5	1 2		0 3	2
6	2 3		0 1	$1+7k$
$49k+$ 1	$7k\pm0$ 2	$49k\pm$ 1	$7k\pm3$	48
2	0 1	10	2	47
4	0 3	2	1	45
8	0 2	20	3	41
9	0 1	3	2	40
11	0 3	16	1	38
15	0 2	8	3	34
16	0 1	4	2	33
18	0 3	19	1	31
22	0 2	13	3	27
23	0 1	11	2	26
25	0 3	5	1	24
29	0 2	15	3	20
30	0 1	18	2	19
32	0 3	9	1	17
36	0 2	6	3	13
37	0 1	24	2	12
39	0 3	23	1	10
43	0 2	22	3	6
44	0 1	17	2	5
46	0 3	12	1	$3+49k$
		y		N

III. — **Valeur** (mod. ρ) **de** a, b, x, y, z, t

dans $a^2 + b^2 = x^2 - y^2 = z^2 + rn^2 = t^2 + nv^2 = N$ (*suite*).

r désigne un résidu quelconque et *n* un non-résidu (mod. ρ).

N.	*a, b, z.*		*x, t.*	
$11k+$ 1	$11k \pm$ 0 3 5	1	2 4	10
2	1 2 3		0 4 5	9
3	0 3 4	5	1 2	8
4	0 1 5	2	3 4	7
5	0 1 2	4	3 5	6
6	1 4 5		0 2 3	5
7	2 3 5		0 1 4	4
8	2 4 5		0 1 3	3
9	0 2 4	3	1 5	2
10	1 3 4		0 2 5	$1 + 11k$
		y		N
N.	*a, b, x, z.*		*t.*	
$13k+$ 1	$13k \pm$ 0 2 6	1	3 4 5	12
2	1 4 5		0 2 3 6	11
3	0 2 5	4	1 3 6	10
4	0 1 4	2	3 5 6	9
5	1 2 3		0 4 5 6	8
6	3 4 6		0 1 2 5	7
7	2 4 6		0 1 3 5	6
8	2 3 5		0 1 4 6	5
9	0 5 6	3	1 2 4	4
10	0 1 3	6	2 4 5	3
11	1 5 6		0 2 3 4	2
12	0 3 4	5	1 2 6	$1 + 13k$
$17k+$ 1	$17k \pm$ 0 3 4 6	1	2 5 7 8	16
2	0 1 2 7	6	3 4 5 8	15
3	1 2 4 6		0 3 5 7 8	14
4	0 5 6 8	2	1 3 4 7	13
5	1 2 3 8		0 4 5 6 7	12
6	2 5 6 7		0 1 3 4 8	11
7	3 4 5 7		0 1 2 6 8	10
8	0 2 3 4	5	1 6 7 8	9
9	0 1 5 8	3	2 3 4 7	8
10	1 3 5 6		0 2 4 7 8	7
11	3 6 7 8		0 1 2 4 5	6
12	2 4 5 8		0 1 3 6 7	5
13	0 2 3 7	8	1 4 5 6	4
14	1 4 7 8		0 2 3 5 6	3
15	0 4 6 8	7	1 2 3 5	2
16	0 1 5 7	4	2 3 6 8	$1 + 17k$
		y		N

III. — **Valeur** (mod. ρ) **de** a, b, x, y, z, t

dans $a^2 + b^2 = x^2 - y^2 = z^2 + rn^2 = t^2 + nv^2 = \mathrm{N}$ (*suite*).

r désigne un résidu quelconque et n un non-résidu (mod. ρ).

N.	a, b, z		$x, t.$	
$19k +$ 1	$19k \pm$ 0 2 3 4 7	1	5 6 8 9	18
2	1 2 4 6 9		0 3 5 7 8	17
3	4 5 6 7 9		0 1 2 3 8	16
4	0 4 5 6 8	2	1 3 7 9	15
5	0 1 2 6 8	9	3 4 5 7	14
6	0 1 3 4 9	5	2 6 7 8	13
7	0 1 3 5 6	8	2 4 7 9	12
8	1 2 4 7 8		0 3 5 6 9	11
9	0 2 6 7 9	3	1 4 5 8	10
10	1 2 3 5 9		0 4 6 7 8	9
11	0 2 5 8 9	7	1 3 4 6	8
12	1 5 7 8 9		0 2 3 4 6	7
13	2 3 4 5 8		0 1 6 7 9	6
14	3 4 6 8 9		0 1 2 5 7	5
15	2 3 5 6 7		0 1 4 8 9	4
16	0 3 7 8 9	4	1 2 5 6	3
17	0 1 4 5 7	6	2 3 8 9	2
18	1 3 6 7 8		0 2 4 5 9	$1 + 19k$
$23k +$ 1	$23k \pm$ 0 4 8 9 10 11	1	2 3 5 6 7	22
2	0 1 3 4 6 9	5	2 7 8 10 11	21
3	0 1 5 6 8 10	7	2 3 4 9 11	20
4	0 1 3 5 7 8	2	4 6 9 10 11	19
5	1 2 4 5 7 9		0 3 6 8 10 11	18
6	0 2 4 5 6 7	11	1 3 8 9 10	17
7	1 2 7 8 9 11		0 3 4 5 6 10	16
8	0 2 5 6 8 11	10	1 3 4 7 9	15
9	0 1 4 7 10 11	3	2 5 6 8 9	14
10	1 2 3 5 10 11		0 4 6 7 8 9	13
11	3 4 5 7 8 10		0 1 2 6 9 11	12
12	0 2 3 7 10 11	9	1 4 5 6 8	11
13	0 1 2 3 8 9	6	4 5 7 10 11	10
14	1 5 6 9 10 11		0 2 3 4 7 8	9
15	3 5 6 7 9 11		0 1 2 4 8 10	8
16	0 2 6 7 9 10	4	1 3 5 8 11	7
17	1 2 3 4 6 10		0 5 7 8 9 11	6
18	0 3 4 5 9 11	8	1 2 6 7 10	5
19	1 4 6 7 8 11		0 2 3 5 9 10	4
20	2 4 5 8 9 10		0 1 3 6 7 11	3
21	3 6 7 8 9 10		0 1 2 4 5 11	2
22	2 3 4 6 8 11		0 1 5 7 9 10	$1 + 23k$
		y		N

III. — **Valeur** (mod. ρ) **de** a, b, x, y, z, t

dans $a^2 + b^2 = x^2 - y^2 = z^2 + rn^2 = t^2 + nv^2 = \mathrm{N}$ (*suite*).

r désigne un résidu quelconque et n un non-résidu (mod. ρ).

N.	$a, b, x, z.$		$t.$	
$29k+$ 1	$29k \pm$ 0 5 6 8 9 11 13	1	2 3 4 7 10 12 14	28
2	1 3 5 6 8 13 14		0 2 4 7 9 10 11 12	27
3	2 3 4 5 6 9 12		0 1 7 8 10 11 13 14	26
4	0 3 7 10 11 12 13	2	1 4 5 6 8 9 14	25
5	0 1 2 3 5 8 12	11	4 6 7 9 10 13 14	24
6	0 1 6 10 11 12 14	8	2 3 4 5 7 9 13	23
7	0 1 4 7 8 9 10	6	2 3 5 11 12 13 14	22
8	1 2 3 6 10 12 13		0 4 5 7 8 9 11 14	21
9	0 2 4 5 10 11 14	3	1 6 7 8 9 12 13	20
10	1 2 3 4 8 9 11		0 5 6 7 10 12 13 14	19
11	2 4 6 7 8 11 13		0 1 3 5 9 10 12 14	18
12	4 5 6 8 10 11 12		0 1 2 3 7 9 13 14	17
13	0 2 3 6 7 8 14	10	1 4 5 9 11 12 13	16
14	1 3 6 7 9 10 11		0 2 4 5 8 12 13 14	15
15	3 4 7 8 12 13 14		0 1 2 5 6 9 10 11	14
16	0 3 5 6 7 9 14	4	1 2 8 10 11 12 13	13
17	1 2 4 9 10 13 14		0 3 5 6 7 8 11 12	12
18	3 5 9 10 11 13 14		0 1 2 4 6 7 8 12	11
19	5 7 8 9 10 12 13		0 1 2 3 4 6 11 14	10
20	0 2 4 5 6 10 13	7	1 3 8 9 11 12 14	9
21	1 4 5 7 11 12 14		0 2 3 6 8 9 10 13	8
22	0 3 4 8 9 10 12	14	1 2 5 6 7 11 13	7
23	0 1 4 6 12 13 14	9	2 3 5 7 8 10 11	6
24	0 1 2 5 7 9 12	13	3 4 6 8 10 11 14	5
25	0 1 3 4 7 11 13	5	2 6 8 9 10 12 14	4
26	1 2 5 7 8 10 14		0 3 4 6 9 11 12 13	3
27	2 6 7 9 11 12 14		0 1 3 4 5 8 10 13	2
28	0 2 8 9 11 13 14	12	1 3 4 5 6 7 10	$1 + 29k$
	y			N

N.	$a, b, z.$		$x, t.$	
$31k+$ 1	$31k \pm$ 0 2 4 5 7 10 11 13	1	3 6 8 9 12 14 15	30
2	0 1 5 6 9 11 13 15	8	2 3 4 7 10 12 14	29
3	1 3 4 5 7 8 12 13		0 2 6 9 10 11 14 15	28
4	0 4 5 8 9 10 11 14	2	1 3 6 7 12 13 15	27
5	0 1 2 4 7 8 12 15	6	3 5 9 10 11 13 14	26
6	1 2 3 6 7 8 9 11		0 4 5 10 12 13 14 15	25
7	0 6 7 8 9 11 12 14	10	1 2 3 4 5 13 15	24
8	0 1 2 5 9 10 12 13	15	3 4 6 7 8 11 14	23
9	0 1 2 6 8 10 12 15	3	4 5 7 9 11 13 14	22
10	0 1 3 4 5 6 8 15	14	2 7 9 10 11 12 13	21
11	1 2 3 8 10 11 13 14		0 4 5 6 7 9 12 15	20
12	2 5 6 7 8 10 14 15		0 1 3 4 9 11 12 13	19
13	2 3 4 5 6 9 11 15		0 1 7 8 10 12 13 14	18
14	0 2 3 5 6 10 12 14	13	1 4 7 8 9 11 15	17
15	1 6 7 10 11 13 14 15		0 2 3 4 5 8 9 12	16
	y			N

III. — **Valeur** (mod. ρ) **de** a, b, x, y, z, t

dans $a^2 + b^2 = x^2 - y^2 = z^2 + rn^2 = t^2 + nv^2 = \text{N}$ (*suite*).

r désigne un résidu quelconque et *n* un non-résidu (mod. ρ).

N.	*a*, *b*, *z*.		*x*. *t*.	
31*k* + 16	31*k* ± 0 3 8 9 10 11 13 15	4	1 2 5 6 7 12 14	15
17	1 3 4 10 11 12 14 15		0 2 5 6 7 8 9 13	14
18	0 2 3 4 8 13 14 15	7	1 5 6 9 10 11 12	13
19	0 1 3 5 6 7 13 14	9	2 4 8 10 11 12 15	12
20	0 1 2 4 7 8 9 14	12	3 5 6 10 11 13 15	11
21	1 4 6 8 9 10 12 13		0 2 3 5 7 11 14 15	10
22	2 5 7 8 11 12 13 15		0 1 3 4 6 9 10 14	9
23	2 3 4 6 7 9 10 13		0 1 5 8 11 12 14 15	8
24	2 4 6 9 12 13 14 15		0 1 3 5 7 8 10 11	7
25	0 3 4 6 7 10 11 12	5	1 2 8 9 13 14 15	6
26	1 4 5 7 9 10 14 15		0 2 3 6 8 11 12 13	5
27	3 5 7 8 9 10 12 15		0 1 2 4 6 11 13 14	4
28	0 3 7 9 12 13 14 15	11	1 2 4 5 6 8 10	3
29	1 2 3 5 9 11 12 14		0 4 6 7 8 10 13 15	2
30	4 5 6 8 11 12 13 14		0 1 2 3 7 9 10 15	1 + 31*k*
	y			N

N.	*a*, *b*, *x*, *z*.		*t*.	
37*k* + 1	37*k* ± 0 2 7 8 10 11 14 16 18	1	3 4 5 6 9 12 13 15 17	36
2	1 3 6 7 8 14 15 17 18		0 2 4 5 9 10 11 12 13 16	35
3	0 2 6 7 9 11 12 17 18	15	1 3 4 5 8 10 13 14 16	34
4	0 1 4 5 9 14 15 16 17	2	3 6 7 8 10 11 12 13 18	33
5	1 2 3 4 7 10 12 13 17		0 5 6 8 9 11 14 15 16 18	32
6	3 4 6 8 9 11 12 15 16		0 1 2 5 7 10 13 14 17 18	31
7	0 2 4 11 12 14 15 16 18	9	1 3 5 6 7 8 10 13 17	30
8	1 2 3 6 7 9 12 14 16		0 4 5 8 10 11 13 15 17 18	29
9	0 4 5 6 7 11 13 16 17	3	1 2 8 9 10 12 14 15 18	28
10	0 1 3 6 9 10 13 14 15	11	2 4 5 7 8 12 16 17 18	27
11	0 1 2 6 7 8 9 11 13	14	3 4 5 10 12 15 16 17 18	26
12	0 1 3 4 12 13 14 15 18	7	2 5 6 8 9 10 11 16 17	25
13	1 2 3 4 5 7 11 15 16		0 6 8 9 10 12 13 14 17 18	24
14	2 5 9 10 11 13 14 15 17		0 1 3 4 6 7 8 12 16 18	23
15	2 4 5 6 7 8 10 14 15		0 1 3 9 11 12 13 16 17 18	22
16	0 2 3 5 7 8 9 10 18	4	1 6 11 12 13 14 15 16 17	21
17	1 4 8 9 10 11 12 13 18		0 2 3 5 6 7 14 15 16 17	20
18	3 5 8 9 13 14 16 17 18		0 1 2 4 6 7 10 11 12 15	19
19	3 4 7 9 10 11 15 17 18		0 1 2 5 6 8 12 13 14 16	18
20	2 3 4 6 8 11 13 14 17		0 1 5 7 9 10 12 15 16 18	17
21	0 3 5 7 11 12 14 17 18	13	1 2 4 6 8 9 10 15 16	16
22	1 5 7 10 11 12 13 14 16		0 2 3 4 6 8 9 15 17 18	15
23	4 7 8 9 10 12 14 16 17		0 1 2 3 5 6 11 13 15 18	14
24	5 6 7 8 12 13 15 16 18		0 1 2 3 4 9 10 11 14 17	13
25	0 2 3 4 6 10 13 16 18	5	1 7 8 9 11 12 14 15 17	12
26	0 1 4 5 6 8 11 12 17	10	2 3 7 9 13 14 15 16 18	11
27	0 1 4 6 10 14 16 17 18	8	2 3 5 7 9 11 12 13 15	10
28	0 1 4 5 7 8 9 13 15	18	2 3 6 10 11 12 14 16 17	9
	y			N

III. — **Valeur** (mod. p) **de** a, b, x, y, z, t

dans $a^2 + b^2 = x^2 - y^2 = z^2 + rn^2 = t^2 + nv^2 = \mathrm{N}$ (*suite*).

r désigne un résidu quelconque et n un non-résidu (mod. d).

N.	$a, b, x, z.$		$t.$	
$37k+29$	$37k\pm$ 1 2 5 6 10 12 15 17 18		0 3 4 7 8 9 11 13 14 16	8
30	0 2 3 8 10 12 13 15 16	17	1 4 5 6 7 9 11 14 18	7
31	1 2 8 11 13 15 16 17 18		0 3 4 5 6 7 9 10 12 14	6
32	2 4 5 6 9 12 13 14 18		0 1 3 7 8 10 11 15 16 17	5
33	0 6 7 9 10 13 15 16 17	12	1 2 3 4 5 8 11 14 18	4
34	0 1 2 3 5 8 9 12 17	16	4 6 7 10 11 13 14 15 18	3
35	1 3 5 6 9 10 11 16 18		0 2 4 7 8 12 13 14 15 17	2
36	0 3 5 8 10 11 12 14 15	6	1 2 4 7 9 13 16 17 18	$1+37k$
$41k+1$	$41k\pm$ 0 3 9 12 13 14 16 17 18 19	1	2 4 5 6 7 8 10 11 15 20	40
2	0 1 2 5 8 10 11 15 16 19	17	3 4 6 7 9 12 13 14 18 20	39
3	1 2 6 7 8 9 11 12 13 17		0 3 4 5 10 14 15 16 18 19 20	38
4	0 3 5 6 7 9 13 15 17 18	2	1 4 8 10 11 12 14 16 19 20	37
5	0 1 2 3 5 6 8 12 16 18	13	4 7 9 10 11 14 15 17 19 20	36
6	1 2 4 7 11 13 16 17 18 20		0 3 5 6 8 9 10 12 14 15 19	35
7	3 4 5 7 8 9 11 13 14 17		0 1 2 6 10 12 15 16 18 19 20	34
8	0 2 3 4 9 10 11 16 19 20	7	1 5 6 8 12 13 14 15 17 18	33
9	0 1 2 5 7 9 10 13 14 16	3	4 6 8 11 12 15 17 18 19 20	32
10	0 1 3 7 10 13 15 17 19 20	16	2 4 5 6 8 9 11 12 14 16 18	31
11	1 3 4 6 12 14 15 16 17 20		0 2 5 7 8 9 10 11 13 18 19	30
12	2 4 7 12 14 15 16 17 18 19		0 1 3 5 6 8 9 10 11 13 20	29
13	2 3 6 7 8 10 12 13 19 20		0 1 4 5 9 11 14 15 16 17 18	28
14	2 3 4 8 10 11 13 14 16 18		0 1 5 6 7 9 12 15 17 19 20	27
15	4 5 6 8 9 13 15 16 19 20		0 1 2 3 7 10 11 12 14 17 18	26
16	0 5 6 7 10 11 12 14 15 18	4	1 2 3 8 9 13 16 17 19 20	25
17	1 3 4 5 7 9 10 12 18 19		0 2 6 8 11 13 14 15 16 17 20	24
18	0 3 4 6 7 8 11 15 16 17	10	1 2 5 9 12 13 14 18 19 20	23
19	1 3 8 9 10 11 12 15 16 18		0 2 4 5 6 7 13 14 17 19 20	22
20	0 2 4 5 6 9 10 12 16 17	15	1 3 7 8 11 13 14 18 19 20	21
21	0 1 4 5 8 11 13 15 18 20	12	2 3 6 7 9 10 14 16 17 19	20
22	1 2 8 9 10 12 14 15 17 20		0 3 4 5 6 7 11 13 16 18 19	19
23	0 5 10 11 12 13 14 17 19 20	8	1 2 3 4 6 7 9 15 16 18	18
24	1 2 4 5 7 8 9 14 15 19		0 3 6 10 11 12 13 16 17 18 20	17
25	0 2 3 4 8 12 13 15 17 19	5	1 6 7 9 10 11 14 16 18 20	16
26	1 4 5 6 7 10 12 13 16 20		0 2 3 8 9 11 14 15 17 18 19	15
27	2 3 5 6 8 10 14 17 18 20		0 1 4 7 9 11 12 13 15 16 19	14
28	6 7 8 10 13 14 15 16 18 19		0 1 2 3 4 5 9 11 12 17 20	13
29	2 3 5 7 11 12 15 18 19 20		0 1 4 6 8 9 10 13 14 16 17	12
30	3 5 9 11 12 13 14 15 16 20		0 1 2 4 6 7 8 10 17 18 19	11
31	0 6 7 8 9 11 12 14 16 19	20	1 2 3 4 5 10 13 15 17 18	10
32	0 1 3 4 6 8 9 18 19 20	14	2 5 7 10 11 12 13 15 16 17	9
33	0 1 5 7 8 14 16 17 18 20	19	2 3 4 6 9 10 11 12 13 15	8
34	1 3 4 5 6 10 11 14 17 19		0 2 7 8 9 12 13 15 16 18 20	7
35	2 5 6 9 11 16 17 18 19 20		0 1 3 4 7 8 10 12 13 14 15	6
36	0 2 4 9 10 13 14 15 18 20	6	1 3 5 7 8 11 12 16 17 19	5
37	0 1 2 4 6 11 12 13 14 19	18	3 5 7 8 9 10 15 16 17 20	4
38	1 6 9 10 11 13 15 17 18 19		0 2 3 4 5 7 8 12 14 16 20	3
39	0 4 7 8 9 10 12 17 18 20	11	1 2 3 5 6 13 14 15 16 19	2
40	0 1 2 3 6 7 11 14 15 20	9	4 5 8 10 12 13 16 17 18 19	$1+41k$
	y			N

III. — **Valeur** (mod. ρ). **de** a, b, x, y, z, t **dans** $a^2+b^2=x^2-y^2=z^2+rn^2=t^2+nv^2=\mathrm{N}$ (*suite*).

r désigne un résidu quelconque et n un non-résidu (mod ρ).

N.	a. b. z.		x, t.	
43k + 1	43k ± 0 2 3 7 8 9 11 13 17 18 20	1	4 5 6 10 12 14 15 16 19 21	42
2	1 2 3 6 8 10 11 14 15 16 17		0 4 5 7 9 12 13 18 19 20 21	41
3	5 6 7 8 11 12 13 15 17 18 21		0 1 2 3 4 9 10 14 16 19 20	40
4	0 3 4 6 7 9 14 16 17 18 21	2	1 5 8 10 11 12 13 15 19 20	39
5	1 2 5 9 11 14 15 17 18 19 20		0 3 4 6 7 8 10 12 13 16 21	38
6	0 3 5 6 9 10 11 13 14 20 21	7	1 2 4 8 12 15 16 17 18 19	37
7	1 3 5 6 7 10 11 12 13 15 16		0 2 4 8 9 14 17 18 19 20 21	36
8	2 4 6 9 11 12 13 15 16 20 21		0 1 3 5 7 8 10 14 17 18 19	35
9	0 4 6 8 9 10 11 16 17 19 21	3	1 2 5 7 12 13 14 15 18 20	34
10	0 1 2 3 6 7 9 12 13 19 20	15	4 5 8 10 11 14 16 17 18 21	33
11	0 1 4 9 10 13 15 16 17 18 20	21	2 3 5 6 7 8 11 12 14 19	32
12	1 7 9 10 12 13 14 16 17 19 21		0 2 3 4 5 6 8 11 15 18 20	31
13	0 2 3 4 5 8 11 12 13 16 17	20	1 6 7 9 10 14 15 18 19 21	30
14	0 1 2 4 6 8 13 15 16 19 20	10	3 5 7 9 11 12 14 17 18 21	29
15	0 1 2 3 7 10 11 16 18 19 21	12	4 5 6 8 9 13 14 15 17 20	28
16	0 1 6 7 8 9 11 12 14 15 18	4	2 3 5 10 13 16 17 19 20 21	27
17	0 1 2 4 5 6 7 11 14 20 21	19	3 8 9 10 12 13 15 16 17 18	26
18	1 2 3 5 6 8 9 10 13 18 19		0 4 7 11 12 14 15 16 17 20 21	25
19	2 3 7 8 9 12 14 15 16 17 20		0 1 4 5 6 10 11 13 18 19 21	24
20	2 3 4 5 7 9 10 13 15 18 21		0 1 6 8 11 12 14 16 17 19 20	23
21	0 2 7 12 13 14 15 16 18 19 21	8	1 3 4 5 6 9 10 11 17 20	22
22	1 3 4 5 7 8 13 14 16 20 21		0 2 6 9 10 11 12 15 17 18 19	21
23	0 3 5 7 10 11 15 16 17 19 20	18	1 2 4 6 8 9 12 13 14 21	20
24	0 1 3 6 10 12 15 17 18 20 21	14	2 4 5 7 8 9 11 13 16 19	19
25	0 1 2 3 4 8 10 12 14 15 21	5	6 7 9 11 13 16 17 18 19 20	18
26	1 3 4 5 9 12 15 17 19 20 21		0 2 6 7 8 10 11 13 14 16 18	17
27	2 4 7 8 10 11 15 18 19 20 21		0 1 3 5 6 9 12 13 14 16 17	16
28	2 6 10 11 12 13 14 17 19 20 21		0 1 3 4 5 7 8 9 15 16 18	15
29	2 4 5 6 7 10 12 16 17 18 20		0 1 3 8 9 11 13 14 15 19 21	14
30	3 4 7 8 9 10 11 12 14 19 20		0 1 2 5 6 13 15 16 17 18 21	13
31	0 4 5 6 7 8 9 10 12 15 19	17	1 2 3 11 13 14 16 18 20 21	12
32	1 3 4 8 11 12 13 17 18 19 21		0 2 5 6 7 9 10 14 15 16 20	11
33	3 4 6 9 11 13 14 15 16 18 19		0 1 2 5 7 8 10 12 17 20 21	10
34	3 5 6 8 14 15 16 18 19 20 21		0 1 2 4 7 9 10 11 12 13 17	9
35	0 2 5 8 9 10 13 14 15 17 21	11	1 3 4 6 7 12 16 18 19 20	8
36	0 1 5 8 9 11 12 16 18 20 21	6	2 3 4 7 10 13 14 15 17 19	7
37	1 4 6 7 8 10 13 14 17 18 20		0 2 3 5 9 11 12 15 16 19 21	6
38	0 5 8 10 12 13 14 16 18 19 20	9	1 2 3 4 6 7 11 15 17 21	5
39	1 2 4 5 9 10 11 12 14 16 18		0 3 6 7 8 13 15 17 19 20 21	4
40	0 2 3 4 5 6 13 14 17 18 19	13	1 7 8 9 10 11 15 16 20 21	3
[illegible]	0 1 4 5 7 11 13 14 15 17 19	16	2 3 6 8 9 10 12 18 20 21	2

	y			N
2	0 1 5 8 13 15 16 17 18 19 20 23	7	2 3 4 6 9 10 11 12 14 21 22	45
3	0 1 4 5 6 7 9 14 18 19 21 22	12	2 3 8 10 11 13 15 16 17 20 23	44
4	0 1 3 7 8 9 11 12 15 18 20 22	2	4 5 6 10 13 14 16 17 19 21 23	43
5	1 2 4 5 6 7 9 11 12 13 20 21		0 3 8 10 14 15 16 17 18 19 22 23	42
6	0 2 4 5 6 7 8 12 13 15 16 19	10	1 3 9 10 14 17 18 20 21 22 23	41
7	0 1 2 6 8 10 11 12 15 18 21 23	17	3 4 5 7 9 13 14 16 19 20 22	40
8	0 1 2 7 9 10 11 13 15 16 17 21	14	3 4 5 6 8 12 18 19 20 22 23	39
9	0 1 7 10 12 13 14 17 18 19 20 22	3	2 4 5 6 8 9 11 15 16 21 23	38
10	1 2 3 5 6 7 10 13 14 16 17 19		0 4 8 9 11 13 15 18 20 21 22 23	37
11	2 3 4 7 9 12 14 15 16 17 18 20		0 1 5 6 8 10 11 13 19 21 22 23	36
12	0 2 3 5 8 9 10 11 12 14 18 19	23	1 4 6 7 13 15 16 17 20 21 22	35
13	1 2 3 6 10 13 17 18 19 20 21 23		0 4 5 7 8 9 11 12 14 15 16 22	34
14	0 5 6 7 9 10 11 14 15 17 20 23	22	1 2 3 4 8 12 13 16 18 19 21	33
15	1 3 5 9 10 12 13 14 15 17 22 23		0 2 4 6 7 8 11 16 18 19 20 21	32
16	0 2 3 6 7 11 14 16 17 18 22 23	4	1 5 8 9 10 12 13 15 19 20 21	31
17	0 1 3 4 6 11 12 13 14 15 19 22	8	2 5 7 9 10 16 17 18 20 21 23	30
18	0 1 2 3 4 7 8 10 13 15 22 23	21	5 6 9 11 12 14 16 17 18 19 20	29
19	1 4 7 8 9 12 17 18 19 20 21 23		0 2 3 5 6 10 11 13 14 15 16 22	28
20	2 4 5 7 8 10 12 14 18 21 22 23		0 1 3 6 9 11 13 15 16 17 19 20	27
21	0 2 3 6 8 9 12 17 19 21 22 23	16	1 4 5 7 10 11 13 14 15 18 20	26
22	1 2 4 10 11 14 15 16 18 19 21 22		0 3 5 6 7 8 9 12 13 17 20 23	25
23	3 4 6 7 8 9 10 13 16 17 18 22		0 1 2 5 11 12 14 15 19 20 21 23	24
24	0 4 8 9 10 12 14 15 16 17 21 23	20	1 2 3 5 6 7 11 13 18 19 22	23
25	0 1 2 3 4 6 8 14 16 17 20 21	5	7 9 10 11 12 13 15 18 19 22 23	22
26	1 3 5 6 7 8 14 15 20 21 22 23		0 2 4 9 10 11 12 13 16 17 18 19	21
27	0 3 5 7 10 12 15 16 18 19 20 21	11	1 2 4 6 8 9 13 14 17 22 23	20
28	0 1 2 4 5 11 12 16 17 20 22 23	13	3 6 7 8 9 10 14 15 18 19 21	19
29	1 2 5 7 8 9 11 13 14 16 18 23		0 3 4 6 10 12 15 17 19 20 21 22	18
30	3 4 7 10 11 12 13 16 20 21 22 23		0 1 2 5 6 8 9 14 15 17 18 19	17
31	2 5 6 8 10 11 12 13 17 18 20 22		0 1 3 4 7 9 14 15 16 19 21 23	16
32	0 2 4 5 13 14 15 17 18 20 21 22	19	1 3 6 7 8 9 10 11 12 16 23	15
33	1 3 4 5 8 10 11 14 16 19 20 23		0 2 6 7 9 12 13 15 17 18 21 22	14
34	0 3 4 5 7 8 10 11 13 17 19 21	9	1 2 6 12 14 15 16 18 19 20 23	13
35	1 8 9 11 12 13 14 16 17 19 21 22		0 2 3 4 5 6 7 10 15 18 20 23	12
36	0 2 3 7 9 11 13 14 19 20 21 23	6	1 4 5 8 10 12 15 16 17 18 22	11
37	0 1 3 4 5 6 9 12 13 16 18 23	15	2 7 8 10 11 14 17 19 20 21 22	10
38	1 2 6 7 8 9 10 15 16 19 20 22		0 3 4 5 11 12 13 14 17 18 21 23	9
39	5 6 7 11 12 15 16 17 19 21 22 23		0 1 2 3 4 8 9 10 13 14 18 20	8
40	2 4 6 9 10 12 13 14 15 19 20 23		0 1 3 5 7 8 11 16 17 18 21 22	7
41	2 3 4 5 8 9 11 15 17 19 20 22		0 1 6 7 10 12 13 14 16 18 21 23	6
42	0 5 6 8 9 10 13 14 16 20 21 22	18	1 2 3 4 7 11 12 15 17 19 23	5
43	1 3 4 5 6 9 10 11 15 17 18 21		0 2 7 8 12 13 14 16 19 20 22 23	4
44	4 6 7 8 11 13 14 15 17 18 19 23		0 1 2 3 5 9 10 12 16 20 21 22	3
45	3 6 8 11 12 13 14 15 16 18 20 21		0 1 2 4 5 7 9 10 17 19 22 23	2
46	2 3 5 9 13 15 16 18 19 21 22 23		0 1 4 6 7 8 10 11 12 14 17 20	$1 + 47k$

III. — Table abrégée des valeurs de x dans $x^2 + Dy^2 = N$.

N.	D = — 1.			
$4k+1$	$2n \pm 1$			
3	0			
$16k+1$	$8n \pm 1$			
3	2			
5	3			
7	$4n+0$			
$32k+5$	$16n \pm 3$			
$64k+1$	$32n \pm 1, 9$			
$256k+1$	$64n \pm 23$	$128n \pm 1, 33$		
$1024k+1$	$64n \pm 23$	$256n \pm 33$	$512n \pm 1, 129$	
$4096k+1$	$64n \pm 23$	$256n \pm 33$	$1024n \pm 129$	$2048n \pm 1, 513$

N.	D = + 1.			
$4k+1$	$2n \pm 1$			
3	–			
$16k+1$	$8n \pm 1$			
3	–			
5	1			
7	–			
$32k+5$	$16n \pm 1$			
$64k+1$	$32n \pm 1, 7$			
$256k+1$	$64n \pm 25$	$128n \pm 1, 31$		
$1024k+1$	$64n \pm 25$	$256n \pm 31$	$512n \pm 1, 127$	
$4096k+1$	$64n \pm 25$	$256n \pm 31$	$1024n \pm 127$	$2048n \pm 1, 511$

N.	D = r.			
$3k+1$	$3n \pm 0\ \ 1$			
2	1			
$9k+1$	$3n$,	$9n \pm 1$		
$81k+1$	$3n$,	$27n \pm 10$,	$81n \pm 1$	
$729k+1$	$3n$,	$27n \pm 10$,	$243n \pm 82$,	$729n \pm 1$
$5k+1$	$5n \pm 0\ \ 1$			
2	1			
$25k+1$	$5n$,	$25n \pm 1$		
$625k+1$	$5n$,	$125n \pm 49, 51$,	$625n \pm 1$	
$7k+1$	$7n \pm 0\ \ 1\ \ 2$			
3	1 3			
$49k+1$	$7n \pm 0\ \ 2$,	$49n \pm 1$		
$11k+1$	$11n \pm 0\ \ 1\ \ 3\ \ 5$			
2	1 2 3			
$121k+1$	$11n \pm 0\ \ 3\ \ 5$,	$121n \pm 1$		

III. — Table abrégée des valeurs de x dans $x^2 + Dy^2 = N$ (*suite*).

N.	D = r (*suite*).
$13k +$ 1 2	$13n \pm$ 0 1 2 6 1 4 5
$17k +$ 1 3	$17n \pm$ 0 1 3 4 6 1 2 4 6
$19k +$ 1 2	$19n \pm$ 0 1 2 3 4 7 1 2 4 6 9
$23k +$ 1 5	$23n \pm$ 0 1 4 8 9 10 11 1 2 4 5 7 9
$29k +$ 1 2	$29n \pm$ 0 1 5 6 8 9 11 13 1 3 5 6 8 13 14
$31k +$ 1 3	$31n \pm$ 0 1 2 4 5 7 10 11 13 1 3 4 5 7 8 12 13
$37k +$ 1 2	$37n \pm$ 0 1 2 7 8 10 11 14 16 18 1 3 6 7 8 14 15 17 18
$41k +$ 1 3	$41n \pm$ 0 1 3 9 12 13 14 16 17 18 19 1 2 6 7 8 9 11 12 13 17
$43k +$ 1 2	$43n \pm$ 0 1 2 3 7 8 9 11 13 17 18 20 1 2 3 6 8 10 11 14 15 16 17
$47k +$ 1 5	$47n \pm$ 0 1 4 6 9 10 11 14 18 19 20 22 23 1 2 4 5 6 7 9 11 12 13 20 21
$53k +$ 1 2	$53n \pm$ 0 1 4 5 8 10 12 13 14 16 19 20 21 22 1 3 7 8 11 12 15 16 18 21 24 25 26
$59k +$ 1 2	$59n \pm$ 0 1 3 5 10 11 13 14 15 17 19 22 23 24 25 29 1 2 4 5 6 7 10 12 16 20 22 23 24 25 29
$61k +$ 1 2	$61n \pm$ 0 1 2 4 7 9 13 14 15 21 22 25 26 27 29 30 1 4 6 7 8 11 12 13 21 23 24 25 26 27 29

III. — Table abrégée des valeurs de x dans $x^2 + Dy^2 = N$ (*suite*).

N.	D = r (*suite*).
$67k+1$ 2	$67n\pm$ 0 1 2 3 7 8 9 10 11 13 14 17 21 26 27 28 30 32 1 2 3 6 9 10 11 12 16 20 22 23 24 25 27 28 30
$71k+1$ 7	$71n\pm$ 0 1 6 8 10 13 14 15 16 18 20 21 23 24 25 29 30 33 35 1 2 7 10 12 14 17 18 19 22 28 29 30 31 32 33 34 35
$73k+1$ 5	$73n\pm$ 0 1 2 3 5 6 7 12 14 16 17 21 24 26 27 29 30 32 36 1 2 3 9 13 15 16 17 18 19 21 22 25 27 28 30 32 36
$79k+1$ 3	$79n\pm$ 0 1 2 4 5 6 7 8 11 14 15 18 23 25 26 27 30 31 32 33 35 1 3 6 8 9 11 14 21 22 25 26 27 28 29 30 33 34 35 36 39
$83k+1$ 2	$83n\pm$ 0 1 3 4 5 6 9 12 13 15 16 17 18 20 25 31 34 35 36 38 40 41 1 2 4 6 7 8 9 10 15 16 18 20 21 22 24 25 28 31 33 37 41
$89k+1$ 3	$89n\pm$ 0 1 3 9 10 13 14 17 19 21 25 27 28 29 30 32 33 34 35 36 41 42 43 1 2 5 9 10 15 19 22 23 24 25 26 28 31 32 33 34 36 38 39 40 44
$97k+1$ 5	$97n\pm$ 0 1 2 3 5 6 7 10 14 16 17 18 20 22 23 26 27 29 32 34 38 39 40 41 48 1 2 3 4 6 7 10 14 19 21 22 24 26 28 30 32 37 38 39 40 41 43 44 47

N.	D = n.
$3k+1$ 2 $9k+1$ $81k+1$ $729k+1$	$3n\pm1$ 0 $9n\pm1$ $27n\pm8$ $81n\pm1$ $27n\pm8$ $243n\pm80$ $729n\pm1$
$5k+1$ 2 $25k+1$ $625k+1$	$5n\pm$ 1 2 0 2 $5n\pm2$ $25n\pm1$ $5n\pm2$ $125n\pm24,26$ $625n\pm1$
$7k+1$ 3 $49k+1$	$7n\pm$ 1 3 0 2 $7n\pm3$ $49n\pm1$
$11k+1$ 2 $121k+1$	$11n\pm$ 1 2 4 0 4 5 $11n\pm$ 2 4 $121n\pm1$

III. — Table abrégée des valeurs de x dans $x^2 + Dy^2 = N$ (*suite*).

N.	D = n (*suite*).
$13k + 1$ 2	$13n \pm$ 1 3 4 5 0 2 3 6
$17k + 1$ 3	$17n \pm$ 1 2 5 7 8 0 3 5 7 8
$19k + 1$ 2	$19n \pm$ 1 5 6 8 9 0 3 5 7 8
$23k + 1$ 5	$23n \pm$ 1 2 3 5 6 7 0 3 6 8 10 11
$29k + 1$ 2	$29n \pm$ 1 2 3 4 7 10 12 14 0 2 4 7 9 10 11 12
$31k + 1$ 3	$31n \pm$ 1 3 6 8 9 12 14 15 0 2 6 9 10 11 14 15
$37k + 1$ 2	$37n \pm$ 1 3 4 5 6 9 12 13 15 17 0 2 4 5 9 10 11 12 13 16
$41k + 1$ 3	$41n \pm$ 1 2 4 5 6 7 8 10 11 15 20 0 3 4 5 10 14 15 16 18 19 20
$43k + 1$ 2	$43n \pm$ 1 4 5 6 10 12 14 15 16 19 21 0 4 5 7 9 12 13 18 19 20 21
$47k + 1$ 5	$47n \pm$ 1 2 3 5 7 8 12 13 14 15 17 21 0 3 8 10 14 15 16 17 18 19 22 23
$53k + 1$ 2	$53n \pm$ 1 2 3 6 7 9 11 15 17 18 23 24 25 26 0 2 4 5 6 9 10 13 14 17 19 20 22 23
$59k + 1$ 2	$59n \pm$ 1 2 4 6 7 8 9 12 16 18 20 21 26 27 28 0 3 8 9 11 13 14 15 17 18 19 21 26 27 28

III. — Table abrégée des valeurs de x dans $x^2 + Dy^2 = N$ (*suite*).

N.	D = n (*suite*).
$61k+1$	$61n \pm$ 1 3 5 6 8 10 11 12 16 17 18 19 20 23 24 28
2	0 2 3 5 9 10 14 15 16 17 18 19 20 22 28 30
$67k+1$	$67n \pm$ 1 4 5 6 12 15 16 18 19 20 22 23 24 25 29 31 33
2	0 4 5 7 8 13 14 15 17 18 19 21 26 29 31 32 33
$71k+1$	$71n \pm$ 1 2 3 4 5 7 9 11 12 17 19 22 26 27 28 31 32 34
7	0 3 4 5 6 8 9 11 13 15 16 20 21 23 24 25 26 27
$73k+1$	$73n \pm$ 1 4 8 9 10 11 13 15 18 19 20 22 23 25 28 31 33 34 35
5	0 4 5 6 7 8 10 11 12 14 20 23 24 26 29 31 33 34 35
$79k+1$	$79n \pm$ 1 3 9 10 12 13 16 17 19 20 21 22 24 28 29 34 36 37 38 39
3	0 2 4 5 7 10 12 13 15 16 17 18 19 20 23 24 31 32 37 38
$83k+1$	$83n \pm$ 1 2 7 8 10 11 14 19 21 22 23 24 26 27 28 29 30 32 33 37 39
2	0 3 5 11 12 13 14 17 19 23 26 27 29 30 32 34 35 36 38 39 40
$89k+1$	$89n \pm$ 1 2 4 5 6 7 8 11 12 15 16 18 20 22 23 24 26 31 37 38 39 40 44
3	0 3 4 6 7 8 11 12 13 14 16 17 18 20 21 27 29 30 35 37 41 42 43
$97k+1$	$97n \pm$ 1 4 8 9 11 12 13 15 19 21 24 25 28 30 31 33 35 36 37 42 43 44 45 46 47
5	0 5 8 9 11 12 13 15 16 17 18 20 23 25 27 29 31 33 34 35 36 42 45 46 48

r désigne un résidu quadratique quelconque.
n désigne un non-résidu quadratique quelconque (mod. N).

Pour avoir les solutions de $x^2 + Dy^2 \equiv R$ (mod. N), R étant un résidu quadratique, on commencera par résoudre la congruence $R \equiv t^2$. On obtiendra les solutions demandées en multipliant celles qui correspondent à $x^2 + Dy^2 \equiv 1$ (mod. N) par t.

De même, ayant les solutions de $x^2 + Dy^2 \equiv N'$ (mod. N), N′ étant un non-résidu, on obtiendra celles de $x^2 + Dy^2 \equiv N''$ (mod. N), N″ étant un autre non-résidu, en multipliant les premières par s, s étant défini par la relation $N'' \equiv N' . s^2$ (mod. N).

Ces tables remplacent donc avantageusement les tables complètes.

IV. — Table de résidus.

1. — *Résidus quadratiques.*

MODULE.	RÉSIDUS.
3....	1
5....	1 4
7....	1 2 4
11....	1 3 4 5 9
13....	1 3 4 9 10 12
17....	1 2 4 8 9 13 15 16
19....	1 4 5 6 7 9 11 16 17
23....	1 2 3 4 6 8 9 12 13 16 18
29....	1 4 5 6 7 9 13 16 20 22 23 24 25 28
31....	1 2 4 5 7 8 9 10 14 16 18 19 20 25 28
37....	1 3 4 7 9 10 11 12 16 21 25 26 27 28 30 33 34 36
41....	1 2 4 5 8 9 10 16 18 20 21 23 25 31 32 33 36 37 39 40
43....	1 4 6 9 10 11 13 14 15 16 17 21 23 24 25 31 35 36 38 40 41
47....	1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42
53....	1 4 6 7 9 10 11 13 15 16 17 24 25 28 29 36 37 38 40 42 43 44 46 47 49 52
59....	1 3 4 5 7 9 12 15 16 17 19 20 21 22 25 26 27 28 29 35 36 41 45 46 48 49 51 53 57
61....	1 3 4 5 9 12 13 14 15 16 19 20 22 25 27 34 36 39 41 42 45 46 47 48 49 52 56 57 58 60
67....	1 4 6 9 10 14 15 16 17 19 21 22 23 24 25 26 29 33 35 36 37 39 40 47 49 54 55 56 59 60 62 64 65
71....	1 2 3 4 5 6 8 9 10 12 15 16 18 19 20 24 25 27 29 30 32 36 37 38 40 43 45 48 49 50 54 57 58 60 64
73....	1 2 3 4 6 8 9 12 16 18 19 23 24 25 27 32 35 36 37 38 41 46 48 49 50 54 55 57 61 64 65 67 69 70 71 72
79....	1 2 4 5 8 9 10 11 13 16 18 19 20 21 22 23 25 26 31 32 36 38 40 42 44 45 46 49 50 51 52 55 62 64 65 67 72 73 76
83....	1 3 4 7 9 10 11 12 16 17 21 23 25 26 27 28 29 30 31 33 36 37 38 40 41 44 48 49 51 59 61 63 64 65 68 69 70 75 77 78 81
89....	1 2 4 5 8 9 10 11 16 17 18 20 21 22 25 32 34 36 39 40 42 44 45 47 49 50 53 55 57 64 67 68 69 71 72 73 78 79 80 81 84 85 87 88
97....	1 2 3 4 6 8 9 11 12 16 18 22 24 25 27 31 32 33 35 36 43 44 47 48 49 50 53 54 61 62 64 65 66 70 72 73 75 79 81 85 86 88 89 91 93 94 95 96
101....	1 4 5 6 9 13 14 16 17 19 20 21 22 23 24 25 30 31 33 36 37 43 45 47 49 52 54 56 58 64 65 68 70 71 76 77 78 79 80 81 82 84 85 87 88 92 95 96 97 100

IV. — **Table de résidus** (*suites*).

1. — *Résidus quadratiques* (suite).

MODULE.	RÉSIDUS.
103....	1 2 4 7 8 9 13 14 15 16 17 18 19 23 25 26 28 29 30 32
	33 34 36 38 41 46 49 50 52 55 56 58 59 60 61 63 64 66 68 72
	76 79 81 82 83 91 92 93 97 98 100
107....	1 3 4 9 10 11 12 13 14 16 19 23 25 27 29 30 33 34 35 36
	37 39 40 41 42 44 47 48 49 52 53 56 57 61 62 64 69 75 76 79
	81 83 85 86 87 89 90 92 99 100 101 102 105
109....	1 3 4 5 7 9 12 15 16 20 21 22 25 26 27 28 29 31 34 35
	36 38 43 45 46 48 49 60 61 63 64 66 71 73 74 75 78 80 81 82
	83 84 87 88 89 93 94 97 100 102 104 105 106 108
113....	1 2 4 7 8 9 11 13 14 15 16 18 22 25 26 28 30 31 32 36
	41 44 49 50 51 52 53 56 57 60 61 62 63 64 69 72 77 81 82 83
	85 87 88 91 95 97 98 99 100 102 104 105 106 109 111 112
127....	1 2 4 8 9 11 13 15 16 17 18 19 21 22 25 26 30 31 32 34
	35 36 37 38 41 42 44 47 49 50 52 60 61 62 64 68 69 70 71 72
	73 74 76 79 81 82 84 87 88 94 98 99 100 103 104 107 113 115 117 120
	121 122 124
131....	1 3 4 5 7 9 11 12 13 15 16 20 21 25 27 28 33 34 35 36
	38 39 41 43 44 45 46 48 49 52 53 55 58 59 60 61 62 63 64 65
	74 75 77 80 81 84 89 91 94 99 100 101 102 105 107 108 109 112 113 114
	117 121 123 125 129
137....	1 2 4 7 8 9 11 14 15 16 17 18 19 22 25 28 30 32 34 36
	37 38 39 44 49 50 56 59 60 61 63 64 65 68 69 72 73 74 76 77
	78 81 87 88 93 98 99 100 101 103 105 107 109 112 115 118 119 120 121 122
	123 126 128 129 130 133 135 136
139....	1 4 5 6 7 9 11 13 16 20 24 25 28 29 30 31 34 35 36 37
	38 41 42 44 45 46 47 49 51 52 54 55 57 63 64 65 66 67 69 71
	77 78 79 80 81 83 86 89 91 96 99 100 106 107 112 113 116 117 118 120
	121 122 124 125 127 129 131 136 137
149....	1 4 5 6 7 9 16 17 19 20 22 24 25 26 28 29 30 31 33 35
	36 37 39 42 45 46 47 49 53 54 61 63 64 67 68 69 73 76 80 81
	82 85 86 88 95 96 100 102 103 104 107 111 112 113 114 116 118 119 120 121
	123 124 125 127 129 130 132 133 140 142 143 144 145 148
151....	1 2 4 5 8 9 10 11 16 17 18 19 20 21 22 25 29 31 32 34
	36 37 38 39 40 42 43 44 45 47 49 50 55 58 59 62 64 68 69 72
	74 76 78 80 81 84 85 86 88 90 91 94 95 97 98 99 100 103 105 110
	116 118 121 123 124 125 127 128 136 137 138 139 144 145 148
157....	1 3 4 9 10 11 12 13 14 16 17 19 25 27 30 31 33 35 36 37
	39 40 42 44 46 47 48 49 51 52 56 57 58 64 67 68 71 75 76 81
	82 86 89 90 93 99 100 101 105 106 108 109 110 111 113 115 117 118 120 121
	122 124 126 127 130 132 138 140 141 143 144 145 146 147 148 153 154 156
163....	1 4 6 9 10 14 15 16 21 22 24 25 26 33 34 35 36 38 39 40
	41 43 46 47 49 51 53 54 55 56 57 58 60 61 62 64 65 69 71 74
	77 81 83 84 85 87 88 90 91 93 95 96 97 100 104 111 113 115 118 119
	121 126 131 132 133 134 135 136 140 143 144 145 146 150 151 152 155 156 158 160
	161

IV. — Table de résidus (*suite*).

I. — *Résidus quadratiques* (suite).

MODULE.	RÉSIDUS.
167....	1 2 3 4 6 7 8 9 11 12 14 16 18 19 21 22 24 25 27 28
	29 31 32 33 36 38 42 44 47 48 49 50 54 56 57 58 61 62 63 64
	65 66 72 75 76 77 81 84 85 87 88 89 93 94 96 97 98 99 100 107
	108 112 114 115 116 121 122 124 126 127 128 130 132 133 137 141 144 147 150 152
	154 157 162
173....	1 4 6 9 10 13 14 15 16 21 22 23 24 25 29 31 33 34 35 36
	37 38 40 41 43 47 49 51 52 54 55 56 57 60 64 67 73 77 78 81
	83 84 85 88 89 90 92 95 96 100 106 109 113 116 117 118 119 121 122 124
	126 130 132 133 135 136 137 138 139 140 142 144 148 149 150 151 152 157 158 159
	160 163 164 167 169 172
179....	1 3 4 5 9 12 13 14 15 16 17 19 20 22 25 27 29 31 36 39
	42 43 45 46 47 48 49 51 52 56 57 59 60 61 64 65 66 67 68 70
	74 75 76 77 80 81 82 83 85 87 88 89 93 95 100 101 106 107 108 110
	116 117 121 124 125 126 129 135 138 139 141 142 144 145 146 147 149 151 153 155
	156 158 161 168 169 171 172 173 177
181....	1 3 4 5 9 11 12 13 14 15 16 20 25 27 29 33 34 36 37 38
	39 42 43 44 45 46 48 49 52 55 56 59 60 62 64 65 67 70 73 75
	79 80 81 82 87 94 99 100 101 102 106 108 111 114 116 117 119 121 122 125
	126 129 132 133 135 136 137 138 139 142 143 144 145 147 148 152 154 156 161 165
	166 167 168 169 170 172 176 177 178 180
191....	1 2 3 4 5 6 8 9 10 12 13 15 16 17 18 20 23 24 25 26
	27 30 32 34 36 39 40 43 45 46 48 49 50 51 52 54 59 60 64 65
	67 68 69 72 75 77 78 79 80 81 85 86 90 92 96 97 98 100 102 103
	104 107 108 109 115 117 118 120 121 125 128 129 130 133 134 135 136 138 144 147
	149 150 153 154 156 158 160 162 163 169 170 172 177 180 184
193....	1 2 3 4 6 7 8 9 12 14 16 18 21 23 24 25 27 28 31 32
	36 42 43 46 48 49 50 54 55 56 59 62 63 64 65 67 69 72 75 81
	83 84 85 86 92 93 95 96 97 98 100 101 107 108 109 110 112 118 121 124
	126 128 129 130 131 134 137 138 139 143 144 145 147 150 151 157 161 162 165 166
	168 169 170 172 175 177 179 181 184 185 186 187 189 190 191 192
197....	1 4 6 7 9 10 15 16 19 22 23 24 25 26 28 29 33 34 36 37
	39 40 41 42 43 47 49 51 53 54 55 59 60 61 62 63 64 65 70 76
	81 83 85 88 90 92 93 96 97 100 101 104 105 107 109 112 114 116 121 127
	132 133 134 135 136 137 138 142 143 144 146 148 150 154 155 156 157 158 160 161
	163 164 168 169 171 172 173 174 175 178 181 182 187 188 190 191 193 196
199....	1 2 4 5 7 8 9 10 13 14 16 18 20 23 25 26 28 29 31 32
	33 35 36 40 43 45 46 47 49 50 51 52 53 56 57 58 61 62 63 64
	65 66 70 72 79 80 81 86 89 90 91 92 94 98 100 102 103 104 106 111
	112 114 115 116 117 121 122 123 124 125 126 128 130 131 132 139 140 144 145 151
	155 157 158 160 161 162 165 169 172 175 177 178 180 182 184 187 188 193 196

IV. — **Table de résidus** (suite).

2. — *Résidus cubiques et sixièmes.*

(Les résidus sixièmes sont aussi résidus cubiques.)

MODULE.	RÉSIDUS CUBIQUES.	RÉSIDUS SIXIÈMES.
7....	6	1
13....	± 5	± 1
19....	8 12 18	1 7 11
31....	15 23 27 29 30	1 2 4 8 16
37....	± 6 8 14	± 1 10 11
43....	2 8 22 27 32 39 42	1 4 11 16 21 35 41
61....	± 8 11 23 24 28	± 1 3 9 20 27
67....	3 5 8 27 42 43 45 52 53 58 66	1 9 14 15 22 24 25 40 59 62 64
73....	± 7 10 17 21 22 30	± 1 3 8 9 24 27
79....	12 14 15 17 27 33 41 57 58 61 69 71 78	1 8 10 18 21 22 38 46 52 62 64 65 67
97....	± 19 20 28 30 34 42 45 46	± 1 8 12 18 22 27 33 47
103....	3 10 22 24 27 31 37 39 42 69 73 80 89 90 94 95 102	1 8 9 13 14 23 30 34 61 64 66 72 76 79 81 93 100
109....	± 2 8 17 19 23 32 33 41 54	± 1 4 16 27 34 38 43 45 46
127....	5 10 20 27 33 40 51 54 63 66 77 80 89 95 102 108 111 119 123 125 126	1 2 4 8 16 19 25 32 38 47 50 61 64 73 76 87 94 100 107 117 122
139....	8 10 14 23 27 33 39 48 59 60 62 74 75 76 82 84 87 94 95 103 105 133 138	1 6 34 36 44 45 52 55 57 63 64 65 77 79 80 91 100 106 112 116 125 129 131
151....	3 24 26 27 28 41 53 57 60 65 67 70 73 79 83 87 92 101 107 122 131 132 142 143 150	1 8 9 19 20 29 44 50 59 64 68 72 78 81 84 86 91 94 98 110 123 124 125 127 148
157....	± 2 7 8 23 28 29 32 41 45 54 59 65 78	± 1 4 14 16 27 39 46 49 56 58 64 67 75
163....	5 8 13 17 23 27 28 30 31 37 48 59 78 86 98 99 102 105 110 123 125 127 138 141 142 157 162	1 6 21 22 25 36 38 40 53 58 61 64 65 77 85 104 115 126 132 133 135 136 140 146 150 155 158
181 ...	± 6 7 8 19 22 26 30 31 35 40 51 68 71 74 86	± 1 5 25 27 29 36 42 46 48 49 56 59 64 67 82
193....	± 11 13 20 29 33 35 39 60 68 71 74 76 87 88 89 94	± 1 3 8 9 14 23 24 27 42 43 50 64 67 69 72 81
199....	11 12 17 27 42 55 59 60 67 74 76 78 82 83 85 88 93 96 101 107 109 135 136 137 138 147 159 171 174 181 191 194 198	1 5 8 18 25 28 40 52 61 62 63 64 90 92 98 103 106 111 114 116 117 121 123 125 132 139 140 144 157 172 182 187 188
211....	8 12 18 23 27 28 40 42 60 63 67 68 86 88 89 90 97 98 102 104 115 124 129 132 135 140 146 147 153 156 186 198 200 206 210	1 5 11 13 25 55 58 64 65 71 76 79 82 87 96 107 109 113 114 121 122 123 125 143 144 148 151 169 171 183 184 188 193 199 203
223....	13 26 27 52 54 59 87 91 95 103 104 108 111 118 125 141 155 157 159 163 167 174 182 189 190 191 193 195 206 207 208 209 215 216 219 221 222	1 2 4 7 8 14 15 16 17 28 30 32 33 34 41 49 56 60 64 66 68 82 98 105 112 115 119 120 128 132 136 164 169 171 196 197 210
229....	± 2 8 13 21 22 30 32 34 52 54 84 86 88 93 101 106 107 109 114	± 1 4 11 15 16 17 26 27 42 43 44 53 57 60 61 64 68 104 108
241....	± 17 21 23 26 28 33 43 44 57 73 76 85 93 101 102 103 105 111 115 117	± 1 5 6 8 25 27 30 36 40 41 47 48 61 64 79 87 91 98 106 116

IV. — Table de résidus (*suite*).

3. — *Résidus biquadratiques.*

MODULE.		RÉSIDUS.
5....		1
13....		1 3 9
17....	±	1 4
29....		1 7 16 20 23 24 25
37....		1 7 9 10 12 16 26 33 34
41....	±	1 4 10 16 18
53....		1 10 13 15 16 24 28 36 42 44 46 47 49
61....		1 9 12 13 15 16 20 22 25 34 42 47 56 57 58
73....	±	1 2 4 8 9 16 18 32 36
89....	±	1 2 4 8 11 16 22 25 32 39 44
97...	±	1 4 6 9 16 22 24 33 35 36 43 47
101....		1 5 16 19 24 25 31 36 37 52 54 56 58 68 71 78 79 80 81 84 87 88 92 95 97
109....		1 3 5 7 9 15 16 21 22 25 26 27 35 38 45 48 49 63 66 73 75 78 80 81 89 97 105
113....	±	1 2 4 7 8 14 15 16 28 30 32 49 53 56
137....	±	1 4 14 15 16 18 22 34 38 49 50 56 59 60 63 64 65
149....		1 5 6 16 17 19 25 28 29 30 31 33 36 37 39 46 49 63 67 73 80 81 85 88 95 96 102 104 107 114 123 125 127 129 140 142 145
157....		1 9 11 12 14 16 17 19 30 35 37 39 40 46 47 52 67 71 75 81 89 93 99 100 101 106 108 109 113 115 121 124 126 130 132 144 147 153 154
173....		1 6 10 14 16 22 23 29 36 43 47 51 52 57 60 81 83 84 85 95 96 100 106 109 117 118 119 124 132 133 135 136 138 139 140 142 148 149 152 158 160 164 169
181....		1 3 5 9 13 14 15 16 25 27 29 34 38 39 42 43 44 45 48 59 62 65 70 73 75 80 81 82 87 102 114 117 121 125 126 129 132 135 144 145 148 161 169 170 177
193....	±	1 3 4 7 9 12 16 21 27 28 36 43 46 48 49 50 55 59 62 63 64 81 84 85
197....		1 16 23 24 28 29 34 36 37 40 42 49 51 53 54 59 60 61 63 70 76 81 85 88 90 100 101 104 105 114 132 133 135 142 150 154 156 158 164 171 172 175 178 182 187 188 190 191 193
229....		1 3 9 14 16 17 19 20 25 27 37 42 43 44 48 51 53 55 57 60 61 75 81 82 83 91 94 104 111 121 126 129 130 132 134 144 149 151 153 158 159 161 165 167 171 173 180 183 184 193 196 203 214 217 218 224 225
233....	±	1 2 4 8 16 19 23 29 32 37 38 46 49 51 58 63 64 71 74 76 81 85 91 92 98 102 105 107 116
241....	±	1 4 6 9 10 15 16 24 25 36 40 54 58 60 64 81 82 83 87 90 91 94 96 97 98 100 106 107 118 119
257....	±	1 2 4 8 11 15 16 17 22 23 30 32 34 35 44 46 60 64 67 68 70 73 81 88 92 95 111 117 120 121 123 128

IV. — **Table de résidus** (*suite*).

4. — Résidus cinquièmes et dixièmes.

(Les résidus dixièmes sont aussi résidus cinquièmes.)

MODULE.	RÉSIDUS CINQUIÈMES.	RÉSIDUS DIXIÈMES.
11....	10	1
31....	6 26 30	1 5 25
41....	± 3 14	± 1 9
61....	± 11 21 32	± 1 13 14
71....	23 26 34 39 41 51 70	1 20 30 32 37 45 48
101....	± 10 32 39 41 44	± 1 6 14 17 36
131....	18 19 24 32 47 51 68 69 71 79 86 92 130	1 39 45 52 60 62 63 80 84 99 107 112 113
151....	23 33 46 66 75 87 92 113 119 132 135 143 147 149 150	1 2 4 8 16 19 32 38 59 64 76 85 105 118 128
181....	± 7 17 19 26 32 61 72 88 89	± 1 39 43 48 49 62 65 73 85
191....	11 14 31 37 38 41 55 66 70 84 122 139 155 159 161 166 185 186 190	1 5 6 25 30 32 36 52 69 107 121 125 136 150 153 154 160 177 180
211....	12 15 26 31 32 33 38 40 50 63 67 88 94 110 138 153 157 168 177 197 210	1 14 34 43 54 58 73 101 117 123 144 148 161 171 173 178 179 180 185 196 199
241....	± 11 19 22 38 44 63 65 76 88 89 111 115	± 1 2 4 8 15 16 30 32 60 64 113 120
251....	2 8 10 32 40 47 50 102 126 128 138 151 157 160 171 182 187 188 200 226 231 235 246 247 250	1 4 5 16 20 25 51 53 54 69 80 91 94 100 113 123 125 149 201 204 211 219 241 243 249
271....	12 13 23 29 33 54 60 65 93 102 111 113 115 127 131 145 146 157 165 183 188 194 239 243 246 266 270	1 5 25 28 32 77 83 88 106 114 125 126 140 144 156 158 160 169 178 206 211 217 238 242 248 258 259
281....	± 6 37 38 47 60 65 73 77 88 89 92 99 113 134	± 1 10 28 32 34 36 39 53 59 79 100 109 116 124
311....	11 41 46 51 61 68 77 86 87 116 142 143 165 171 185 190 198 206 220 222 228 262 264 279 287 291 293 296 298 304 310	1 7 13 15 18 20 24 32 47 49 83 89 91 105 113 121 126 140 146 168 169 195 224 225 234 243 250 260 265 270 300
331....	13 23 32 34 38 47 48 51 57 61 72 108 112 119 133 151 162 164 168 185 199 200 211 220 236 242 243 246 251 252 257 300 330	1 31 74 79 80 85 88 89 95 111 120 131 132 146 163 167 169 180 198 212 219 223 259 270 274 280 283 284 293 297 299 308 318
401....	± 26 30 33 48 68 76 84 108 119 133 142 147 148 153 155 157 158 171 189 199	± 1 20 22 29 32 35 39 45 56 72 83 98 102 114 126 151 162 164 179 188
421....	± 6 29 32 52 70 95 110 111 115 120 126 137 159 170 171 188 195 198 202 205 207	± 1 20 21 33 36 51 75 86 93 109 112 122 135 149 152 174 176 178 182 184 192

IV. — Table de résidus (*suite*).

5. — *Résidus septièmes et quatorzièmes.*

(Les résidus quatorzièmes sont aussi résidus septièmes.)

MODULE.	RÉSIDUS SEPTIÈMES.	RÉSIDUS QUATORZIÈMES.
29....	± 12	± 1
43...	7 37 42	1 6 36
71....	14 17 46 66 70	1 5 25 54 57
113....	± 35 40 42 48	± 1 15 18 44
127....	20 24 28 59 75 90 105 108 126	1 19 22 37 52 68 99 103 107
197....	± 14 20 68 69 77 84 87	± 1 6 19 33 36 83 93
211....	10 15 23 61 74 77 104 111 128 140 156 190 192 197 210	1 14 19 21 55 71 83 100 107 134 137 150 188 196 201
239....	23 28 52 73 76 107 111 138 164 168 172 188 199 203 217 233 238	1 6 22 36 40 51 67 71 75 101 128 132 163 166 187 211 216
281....	± 60 61 67 89 93 102 129 130 135 139	± 1 7 40 49 53 62 68 86 90 128
337....	± 30 38 40 59 65 105 133 138 140 146 153 163	± 1 54 72 85 96 111 117 128 129 148 156 165
379....	11 40 52 69 85 108 111 128 140 145 166 182 186 194 199 202 228 258 264 272 292 295 300 318 328 355 378	1 24 51 61 79 84 87 107 115 121 151 177 180 185 193 197 213 234 239 251 268 271 294 310 327 339 368
421....	± 13 29 34 73 92 128 148 151 156 159 161 162 173 188 197	± 1 12 20 21 35 38 44 67 77 82 107 142 144 169 181
449....	± 24 37 52 58 71 79 84 95 108 131 155 182 188 203 209 215	± 1 10 22 35 45 67 77 92 99 100 102 122 127 128 221 229
463....	6 22 38 90 93 101 107 126 148 170 216 234 235 238 269 284 305 320 329 330 331 335 341 368 369 386 395 408 424 427 442 448 462	1 15 21 36 39 55 68 77 94 95 122 128 132 133 134 143 158 179 194 225 228 229 247 293 315 337 356 362 370 373 425 441 457
491....	63 66 91 105 110 128 136 159 162 175 186 234 236 251 259 261 265 268 270 278 283 294 301 308 310 338 347 353 377 390 435 450 471 479 490	1 12 20 41 56 101 114 138 144 153 181 183 190 197 208 213 221 223 226 230 232 240 255 257 305 316 329 332 355 363 381 386 400 425 428
547....	26 28 30 38 41 59 72 83 102 106 107 128 145 172 194 197 222 245 251 254 286 308 310 314 316 330 348 366 411 418 426 451 493 500 501 507 526 536 546	1 11 21 40 46 47 54 96 121 129 136 181 199 217 231 233 237 239 261 293 296 302 325 350 353 375 402 419 440 441 445 464 475 488 506 509 517 519 521
617....	± 10 29 46 73 89 101 104 139 150 182 185 192 205 218 228 234 262 281 282 286 291 307	± 1 15 31 69 100 113 128 152 156 157 175 188 194 199 224 225 265 266 273 275 288 290
631....	11 22 44 69 73 88 119 138 146 147 175 176 238 255 276 287 292 294 315 321 350 352 375 389 403 443 459 473 476 503 510 517 537 545 552 567 574 584 588 599 615 623 627 629 630	1 2 4 8 16 32 43 47 57 64 79 86 94 114 121 128 155 158 172 188 228 242 256 279 281 310 316 337 339 344 355 376 393 455 456 484 485 493 512 543 558 562 587 609 620

IV. — Table de résidus (*suite*).

6. — *Résidus huitièmes et seizièmes.*

(Les résidus seizièmes sont aussi résidus huitièmes.)

MODULE.	RÉSIDUS HUITIÈMES.	RÉSIDUS SEIZIÈMES.
17....	16	1
41....	1 10 16 18 37	–
73....	1 2 4 8 16 32 37 55 64	–
89....	1 2 4 8 16 32 39 45 64 67 78	–
97....	± 6 16 22	± 1 35 36
113....	4 7 64 83 85 97 112	1 16 28 30 49 106 109
137....	1 16 34 38 50 56 59 60 72 73 74 88 115 119 122 123 133	–
193....	± 7 9 12 16 43 55	± 1 49 63 81 84 85
233....	1 2 4 8 16 19 23 32 37 38 46 51 63 64 71 74 76 92 102 117 126 128 135 142 148 152 175 184 204	–
241...	10 16 36 58 81 122 141 143 147 150 154 187 217 226 240	1 15 24 54 87 91 94 98 100 119 160 183 205 225 231
257....	± 15 17 30 34 60 68 120 121	± 1 2 4 8 16 32 64 128
281....	1 4 16 35 50 58 59 63 64 79 85 86 90 98 101 109 111 123 140 153 155 162 163 165 181 200 211 232 236 238 249 252 256 273 279	–
313....	1 3 9 16 26 27 44 48 50 58 76 78 81 83 98 103 113 119 121 132 137 142 144 150 174 205 209 214 228 234 243 249 256 277 280 294 301 302 309	–
337....	21 42 81 84 129 162 168 179 209 233 258 273 285 305 311 321 324 329 333 335 336	1 2 4 8 13 16 26 32 52 64 79 104 128 158 169 175 208 253 256 295 316
353....	± 4 34 35 42 64 88 121 135 146 162 171	± 1 16 22 58 97 122 131 136 140 166 169
401....	14 16 29 31 70 80 83 86 145 146 177 205 206 223 228 276 313 324 329 338 350 362 376 396 400	1 5 25 39 51 63 72 77 88 125 173 178 195 196 224 255 256 315 318 321 331 360 372 385 387
409....	1 5 6 16 17 25 30 36 53 69 71 77 80 81 82 83 85 89 96 98 101 102 125 133 139 150 167 179 180 184 197 203 216 218 256 262 265 272 286 289 309 318 341 345 355 363 364 385 389 400 405	–
433....	16 48 59 98 137 144 164 177 190 199 235 272 280 283 294 352 355 367 382 383 406 407 411 416 424 430 432	1 3 9 17 22 26 27 50 51 66 78 81 139 150 153 161 198 234 243 256 269 289 296 335 374 385 417

IV. — Table de résidus (*suite*).

7. — *Résidus neuvièmes et dix-huitièmes.*

(Les résidus dix-huitièmes sont aussi résidus neuvièmes.)

MODULE.	RÉSIDUS NEUVIÈMES.	RÉSIDUS DIX-HUITIÈMES.
19....	18	1
37....	± 6	± 1
73....	± 10 22	± 1 27
109....	± 8 33 41	± 1 45 46
127....	63 95 111 119 123 125 126	1 2 4 8 16 32 64
163....	23 30 59 78 105 110 123 125 162	1 38 40 53 58 85 104 133 140
181....	± 19 22 31 35 74	± 1 42 46 56 59
199 ...	11 60 74 78 85 96 136 137 138 181 198	1 18 61 62 63 103 114 121 125 139 188
271....	3 19 27 29 30 84 171 181 184 190 214 243 261 262 270	1 9 10 28 57 81 87 90 100 187 241 242 244 252 268
307....	3 8 27 34 35 38 72 91 192 193 202 205 226 243 283 298 306	1 9 24 64 81 102 105 114 115 216 235 269 272 273 280 299 304
379....	52 57 68 124 133 162 163 184 241 254 260 285 286 288 293 303 328 340 354 374 378	1 5 25 39 51 76 86 91 93 94 119 125 138 195 216 217 246 255 311 322 327
397....	± 2 8 32 62 63 115 128 145 149 183 198	± 1 4 16 31 64 99 107 124 126 141 167
433....	± 21 45 73 77 91 138 151 165 168 172 183 195	± 1 8 54 64 79 115 133 140 148 179 198 199
487....	5 12 44 95 125 126 186 195 203 205 228 233 255 267 296 300 321 343 344 349 427 436 446 448 462 468 486	1 19 25 39 41 51 60 138 143 144 166 187 191 220 232 254 259 282 284 292 301 361 362 392 443 475 482
523....	3 27 33 50 58 95 115 129 136 155 178 219 238 243 297 317 332 349 363 373 389 402 424 442 450 480 512 514 522	1 9 11 43 73 81 99 121 134 150 160 174 191 206 226 280 285 304 345 368 387 394 408 428 465 473 490 496 520
541....	± 17 29 44 46 52 56 89 120 191 209 216 231 247 266 268	± 1 48 110 115 124 129 130 140 194 198 207 228 234 241 252
577....	± 20 37 42 67 78 83 97 123 141 146 155 202 232 258 261 266	± 1 24 27 33 35 65 71 127 152 163 171 177 186 209 215 263
613....	± 24 35 59 69 93 101 107 145 152 176 187 231 237 246 269 275 281	± 1 27 28 30 37 67 116 143 171 183 190 197 198 220 226 227 287
631....	6 30 38 52 106 119 122 126 150 167 190 204 216 260 319 333 352 362 389 403 412 449 451 461 498 506 526 530 548 595 597 606 610 626 630	1 15 21 25 34 36 83 101 105 125 133 170 180 182 219 228 242 269 279 298 312 371 415 427 441 464 481 505 509 512 525 579 593 601 625
739....	8 47 50 52 97 108 109 127 129 160 198 201 244 252 261 265 296 301 323 325 338 339 356 363 372 446 456 462 469 512 548 588 606 609 614 633 675 682 702 719 738	1 20 37 57 64 106 125 130 133 151 191 227 270 277 283 293 367 376 383 400 401 414 416 438 443 474 478 487 495 538 541 579 610 612 630 631 642 687 689 692 731

V. — Table des indices de tous les nombres premiers inférieurs à 50 pour tous les modules inférieurs à 1000.

N.	N — 1	ρ.	2.	3.	5.	7.	11.	13.	17.	19.	23.	29.	31.	37.	41.	43.	47.
2.....	1		–														
3.....	2	2	1	–													
5.....	4	2	1	3	–												
7.....	2.3	3	2	1	5	–											
11.....	2.5	2	1	8	4	7	–										
13.....	4.3	6	5	8	9	7	11	–									
17.....	16	10	10	11	7	9	13	12	–								
19.....	2.9	10	17	5	2	12	6	13	8	–							
23.....	2.11	10	8	20	15	21	3	12	17	5	–						
29.....	4.7	10	11	27	18	20	23	2	7	15	24	–					
31.....	2.3.5	17	12	13	20	4	29	23	1	22	21	27	–				
37.....	4.9	5	11	34	1	28	6	13	5	25	21	15	27	–			
41.....	8.5	6	26	15	22	39	3	31	33	9	36	7	28	32	–		
43.....	2.3.7	28	39	17	5	7	6	40	16	29	20	25	32	35	18	–	
47.....	2.23	10	30	18	17	38	27	3	42	29	39	43	5	24	25	37	–
53.....	4.13	26	25	9	31	38	46	28	42	41	39	6	45	22	33	30	8
59.....	2.29	10	25	32	34	44	45	23	14	22	27	4	7	41	2	13	53
61.....	4.3.5	10	47	42	14	23	45	20	49	22	39	25	13	33	18	41	40
67.....	2.3.11	12	29	9	39	7	61	23	8	26	20	22	43	44	19	63	64
71.....	2.5.7	62	58	18	14	33	43	27	7	38	5	4	13	30	55	44	17
73....	8.9	5	8	6	1	33	55	59	21	62	46	35	11	64	4	51	31
79.....	2.3.13	29	50	71	34	19	70	74	9	10	52	1	76	23	21	47	55
83.....	2.41	50	3	52	81	24	72	67	4	59	16	36	32	60	38	49	69
89.....	8.11	30	72	87	18	7	4	65	82	53	31	29	57	77	67	59	34
97.....	32.3	10	86	2	11	53	82	83	19	27	79	47	26	41	71	44	60
101.....	4.25	2	1	69	24	9	13	66	30	96	86	91	84	56	45	42	58
103.....	2.3.17	6	46	57	59	32	29	66	50	28	90	76	99	81	94	55	17
107.....	2.53	63	95	78	13	57	76	58	105	96	60	72	21	6	90	93	16
109.....	4.27	10	93	28	16	88	107	7	21	3	105	10	74	65	45	66	5
113.....	16.7	10	52	79	61	72	22	58	59	93	103	87	30	29	34	17	97
127.....	2.9.7	109	18	23	111	125	52	20	118	42	11	79	50	112	76	121	120
131.....	2.5.13	10	83	126	48	38	98	64	59	45	89	73	67	23	58	22	5
137.....	8.17	12	130	13	23	2	90	53	86	54	129	95	133	102	51	37	111
139.....	2.3.23	92	119	49	22	16	74	26	37	83	39	8	40	136	82	23	70
149.....	4.37	10	117	115	32	38	25	133	4	60	15	128	52	136	61	77	14
151.....	2.3.25	114	70	141	82	37	34	101	88	90	115	54	58	76	111	38	86
157.....	4.3.13	139	147	122	11	57	152	130	128	116	81	15	58	28	75	151	76
163.....	2.81	70	71	43	93	161	97	57	159	127	153	145	39	75	20	106	160
167.....	2.83	10	86	144	81	96	110	43	143	50	51	32	152	127	55	75	68
173.....	4 43	91	13	7	163	31	127	142	89	85	88	152	122	42	74	60	144
179.....	2.89	10	73	52	106	23	27	134	14	26	65	70	76	19	101	144	136
181.....	4.9.5	10	133	68	48	15	146	32	55	135	29	84	27	38	59	140	109
191.....	2.5.19	157	102	148	90	133	115	156	184	93	112	29	125	65	145	174	39
193.....	64.3	10	182	156	11	184	93	15	149	59	54	9	134	55	125	72	127
197.....	4.49	73	61	65	137	86	5	153	95	182	68	40	173	148	46	54	106
199.....	2.9.11	197	194	155	6	32	189	128	57	11	74	158	76	121	145	176	98
211.....	2.3.5.7	142	169	127	48	181	78	186	31	196	189	11	115	202	143	80	166
223.....	2.3.37	10	18	137	205	132	7	159	192	32	131	220	134	178	198	182	190
227.....	2.113	217	179	98	161	220	40	71	93	222	210	76	7	223	171	182	150
229.....	4.3.19	10	27	224	202	181	78	183	12	64	227	143	211	44	217	120	49

V. — Table des indices de tous les nombres premiers inférieurs à 50 pour tous les modules inférieurs à 1000 (*suite*).

N.	N — 1.	ρ.	2.	3.	5.	7.	11.	13.	17.	19.	23.	29.	31.	37.	41.	43.	47.
233.....	8.29	10	200	93	33	230	225	78	67	120	208	212	222	48	17	5	167
239.....	2.7.17	237	120	48	186	229	202	89	8	33	147	226	212	197	61	103	173
241.....	16.3.5	112	110	22	138	41	65	7	231	125	177	74	191	113	6	99	114
251.....	2.125	224	195	42	60	26	7	134	38	131	188	171	82	59	198	39	95
257.....	256	10	80	87	177	227	156	6	200	123	132	242	62	109	117	89	187
263.....	2.131	10	156	110	107	69	208	84	120	147	186	67	142	112	247	234	143
269.....	4.67	10	109	89	160	195	146	202	189	187	156	15	91	208	92	82	4
271.....	2.27.5	269	136	63	80	178	112	165	266	171	15	225	12	22	96	101	183
277.....	4.3.23	199	57	148	83	170	29	210	269	216	152	70	37	45	246	149	154
281.....	8.5.7	117	44	51	246	42	23	179	66	71	247	92	82	165	53	12	185
283.....	2.3.47	273	195	191	229	82	268	10	193	57	206	222	149	271	26	213	37
293.....	4.73	204	47	79	247	83	149	33	120	253	93	223	118	23	189	58	169
307.....	2.9.17	297	237	9	223	164	280	115	204	132	137	203	161	28	74	235	47
311.....	2.5.31	301	84	288	72	140	135	80	187	269	221	117	309	263	245	171	210
313.....	8.3.13	10	274	56	39	123	148	214	205	108	27	182	211	163	209	13	37
317.....	4.79	270	147	263	13	82	308	99	109	301	100	155	80	62	183	32	159
331.....	2.3.5.11	140	319	49	14	9	113	175	106	26	265	79	220	221	247	208	145
337.....	16.3.7	10	304	314	33	318	171	16	9	109	229	257	101	148	220	78	96
347.....	2.173	337	145	242	29	39	342	256	239	265	47	160	218	219	3	326	71
349.....	4.3.29	220	253	314	98	247	93	7	198	236	268	50	144	210	324	209	183
353.....	32.11	212	12	131	351	297	116	147	300	18	82	20	215	289	138	50	46
359.....	2.179	349	280	346	258	75	286	339	38	319	288	275	149	106	204	301	272
367.....	2.3.61	10	322	99	45	294	181	76	157	119	176	291	34	98	124	125	330
373.....	4.3.31	291	151	226	223	138	167	198	54	357	177	104	30	38	36	209	145
379.....	2.27.7	10	73	173	306	353	343	169	79	304	240	93	223	156	222	251	143
383.....	2.191	10	250	160	133	358	141	197	120	100	248	22	54	5	97	180	181
389.....	4.97	10	105	131	284	296	212	256	292	350	201	279	145	155	38	37	135
397.....	4.9.11	28	45	94	155	307	316	211	87	40	250	232	328	280	11	210	68
401.....	16.25	211	98	173	304	326	362	387	259	199	343	280	111	309	344	278	114
409.....	8.3.17	235	194	94	216	187	69	33	344	333	242	325	51	329	406	279	193
419.....	2.11.19	10	49	302	370	66	269	266	29	309	344	360	139	340	394	268	330
421.....	4.3.5.7	238	137	328	286	162	272	231	122	129	419	105	352	237	59	233	321
431.....	2.5.43	421	360	380	286	373	254	371	383	402	338	54	77	131	322	429	105
433.....	16.27	10	258	16	175	371	286	430	208	295	221	67	235	186	4	231	185
439.....	2.3.73	429	150	33	70	42	356	50	271	226	143	416	97	175	415	65	315
443.....	2.13.17	433	421	394	243	369	435	182	60	293	301	405	219	90	386	181	76
449.....	64.7	3	254	1	96	44	264	115	347	177	108	425	23	259	438	51	143
457.....	8.3.19	380	90	50	369	244	441	161	396	364	413	340	307	159	383	375	158
461.....	4.5.23	10	169	359	292	71	321	395	242	116	60	143	147	235	370	376	257
463.....	2.3.7.11	174	82	247	383	369	457	187	116	107	393	134	376	389	185	8	366
467.....	2.233	457	405	44	295	292	253	34	384	159	352	55	299	197	202	196	276
479.....	2.239	469	206	370	34	144	50	93	53	105	376	297	185	113	267	287	261
487.....	2.243	10	442	349	45	417	97	47	11	414	361	294	388	15	270	33	253
491.....	2.5.49	10	13	240	478	367	48	396	80	321	167	423	426	340	224	200	361
499.....	2.3.83	10	3	453	496	79	347	27	391	217	227	314	192	135	367	430	64
503.....	2.251	10	320	436	183	176	156	102	241	199	462	11	151	123	335	30	340
509.....	4.127	10	67	95	442	305	502	367	412	357	288	110	353	326	437	76	207
521.....	8.5.13	439	478	201	52	131	98	334	147	51	457	160	12	372	303	195	78
523.....	2.9.29	513	47	387	215	274	162	292	426	406	478	484	190	155	492	54	11
541.....	4.5.27	10	113	412	428	534	395	449	387	334	184	207	530	347	160	488	86

V. — Table des indices de tous les nombres premiers inférieurs à 50 pour tous les modules inférieurs à 1000 (*suite*).

N.	N — 1.	ρ.	2.	3.	5.	7.	11.	13.	17.	19.	23.	29.	31.	37.	41.	43.	47.
547.....	2.3.7.13	17	499	39	323	73	532	208	1	110	425	342	501	43	91	283	56
557.....	4.139	41	171	437	387	478	367	115	94	232	271	98	67	181	1	56	255
563.....	2.281	553	453	116	391	442	310	140	308	44	240	135	549	9	539	485	102
569.....	8.71	420	410	179	160	546	509	554	258	387	269	97	25	333	340	300	13
571.....	2.3.5.19	10	155	313	416	483	94	166	449	541	48	470	240	176	245	172	145
577.....	64.9	10	260	228	317	529	78	7	446	12	490	543	160	81	303	421	123
587.....	2.293	577	229	466	65	124	255	111	498	31	501	480	198	321	51	178	456
593.....	16.37	10	132	75	461	209	235	81	54	468	248	244	92	360	423	401	201
599.....	2.13.23	589	282	314	18	453	289	388	392	414	227	131	185	222	198	177	490
601.....	8.3.25	506	552	344	50	11	527	570	535	251	122	101	297	580	169	37	32
607.....	2.3.101	575	182	157	427	42	332	76	355	302	359	589	497	159	568	506	288
613.....	4.9.17	32	245	390	67	392	487	341	260	372	177	14	447	108	400	156	210
617.....	8.7.11	410	92	491	531	114	534	487	289	214	559	595	392	386	610	508	404
619.....	2.3.103	10	479	81	140	322	485	615	129	253	236	525	138	490	428	255	513
631.....	2.9.5.7	621	532	179	414	271	301	169	422	269	94	68	398	425	590	210	364
641.....	128.5	3	470	1	230	134	516	352	633	407	207	615	565	628	271	69	29
643.....	2.3.107	353	57	114	267	10	533	61	617	313	518	640	458	413	475	87	545
647.....	2.17.19	10	66	112	581	74	643	176	622	281	229	484	592	637	606	342	503
653.....	4.163	140	67	341	587	584	174	78	235	608	290	361	120	633	73	251	588
659.....	2.7.47	10	149	78	510	467	430	632	246	566	152	295	231	162	469	357	371
661.....	4.3.5.11	284	17	450	646	645	520	201	26	63	337	130	558	389	248	622	118
673.....	32.3.7	198	14	236	661	30	187	104	671	359	432	154	271	552	279	169	517
677.....	4.169	213	103	665	575	409	25	404	457	225	413	603	447	282	324	289	51
683.....	2.11.31	673	403	330	621	203	161	551	205	580	213	376	459	165	401	373	295
691.....	2.3.5.23	521	27	167	666	328	55	217	343	285	175	418	597	626	541	404	212
701.....	4.25.7	10	459	211	242	348	257	308	690	400	395	404	34	59	578	222	465
709.....	4.3.59	10	491	200	218	44	458	15	191	116	269	112	5	221	637	50	210
719.....	2.359	709	558	60	520	108	463	492	153	469	235	296	24	686	509	305	445
727.....	2.3.121	10	426	555	301	574	417	326	586	119	432	187	205	625	333	266	350
733.....	4.3.61	583	657	280	447	697	63	341	82	618	655	711	8	400	694	209	186
739.....	2.9.41	730	393	185	348	311	146	501	176	445	65	377	460	342	344	634	405
743.....	2.7.53	10	674	682	69	79	482	505	465	600	48	45	264	378	628	452	152
751.....	2.3.125	39	574	389	554	489	635	362	481	2	698	203	253	58	135	96	704
757.....	4.27.7	2	1	84	139	124	92	356	452	698	581	105	647	689	151	283	513
761.....	8.5.19	422	62	115	700	611	377	75	714	254	710	94	33	282	38	543	362
769.....	256.3	78	622	16	150	759	5	131	678	704	367	565	338	323	68	264	110
773.....	4.193	302	103	619	285	583	34	245	716	37	419	75	305	548	685	203	404
787.....	2.3.131	777	173	669	221	578	722	521	515	88	712	304	180	326	38	189	500
797.....	4.199	623	371	321	29	697	264	92	786	203	387	503	179	151	412	568	381
809.....	8.101	703	266	201	546	216	579	194	567	300	174	261	145	509	309	498	649
811.....	2.81.5	10	327	101	484	510	578	269	695	546	649	456	293	6	684	692	465
821.....	4.5.41	10	607	567	214	26	219	677	89	168	138	304	727	430	622	636	327
823.....	2.3.137	10	700	571	123	439	705	230	767	591	47	99	248	148	281	269	671
827.....	2.7.59	817	589	452	651	29	74	421	157	478	396	309	710	171	265	349	58
829.....	4.9.23	598	187	760	644	87	396	466	200	145	176	153	765	407	88	575	149
839.....	2.419	829	114	14	306	176	83	749	195	122	246	57	491	834	7	494	34
853.....	4.3.71	394	53	414	375	435	655	105	37	554	242	47	248	237	162	806	832
857.....	8.107	10	690	163	167	515	813	46	775	625	316	758	630	109	702	328	225
859.....	2.3.11.13	2	1	119	362	634	387	780	800	689	649	763	460	641	106	494	112
863.....	2.431	10	142	338	721	183	839	695	404	322	375	706	254	678	52	626	17

V. — Table des indices de tous les nombres premiers inférieurs à 50 pour tous les modules inférieurs à 1000 (*suite*).

N.	N — 1.	ρ.	2.	3.	5.	7.	11.	13.	17.	19.	23.	29.	31.	37.	41.	43.	47.
877.....	4.3.73	42	187	386	691	304	699	779	27	737	776	354	532	628	496	276	11
881.....	16.5.11	115	624	359	258	649	326	634	237	722	623	405	57	178	58	822	5
883.....	2.9.49	873	659	791	665	423	577	626	702	817	547	716	156	543	463	769	507
887.....	2.443	10	52	178	835	878	278	358	159	398	351	423	745	552	683	38	718
907.....	2.3.151	539	337	661	119	875	63	236	461	828	12	757	707	515	172	497	837
911.....	2.5.7.13	901	870	524	496	845	595	64	223	546	672	423	476	723	38	786	7
919.....	2.27.17	909	132	345	328	647	908	42	210	233	194	30	103	739	547	913	400
929.....	32.29	224	318	131	612	267	42	907	723	712	88	730	795	804	497	363	650
937.....	8.9.13	10	152	604	785	667	505	676	266	826	429	916	530	742	327	551	451
941.....	4.5.47	10	677	831	264	477	231	801	543	457	423	706	809	770	254	296	732
947.....	2.11.43	937	285	340	189	495	463	347	731	623	449	617	390	843	591	671	209
953. ...	8.7.17	10	518	941	435	676	387	46	150	29	767	660	301	366	662	247	3
967.....	2.3.7.23	526	88	141	881	101	834	293	174	739	153	477	356	17	735	769	815
971.....	2.5.97	10	685	308	286	450	339	490	876	956	298	3	243	896	67	33	42
977.....	16.61	10	630	891	347	618	678	509	626	861	3	526	40	587	765	196	260
983.....	2.491	10	500	374	483	182	415	651	3	796	420	853	212	878	90	454	444
991.....	2.9.5.11	981	272	249	224	109	491	886	705	304	313	732	620	69	529	454	681
997.....	4.3.83	656	105	18	897	169	625	412	947	908	730	71	870	51	577	733	317
$N = \alpha^n$.	$\varphi(N)$.																
$9 = 3^2$	3.2	2	1	–	5	4	–										
$25 = 5^2$	5.4	2	1	7	–	5	16	19	13	18	11	–					
$27 = 3^3$	9.2	2	1	–	5	16	13	8	15	12	11	–					
$49 = 7^2$	7.2.3	3	26	1	29	–	40	33	25	35	38	18	7	32	15	6	5
$81 = 3^4$	27.2	2	1	–	23	16	13	8	33	48	11	37	20	42	53	22	7
$121 = 11^2$	11.2.5	2	1	88	74	7	–	101	49	83	70	17	86	42	23	25	98
$125 = 5^3$	25.4	2	1	7	–	85	76	39	73	18	31	62	48	29	44	95	97
$169 = 13^2$	13.4.3	2	1	124	9	107	103	–	146	65	130	40	21	151	85	122	63
$243 = 3^5$	81.2	2	1	–	23	70	121	8	33	156	65	37	20	96	53	130	61
$289 = 17^2$	17.16	3	190	1	229	155	23	196	–	14	223	125	9	129	171	226	100
$343 = 7^3$	49.2.3	3	194	1	29	–	208	285	25	245	164	228	133	74	183	6	215
$361 = 19^2$	19.2.9	2	1	139	232	150	102	329	226	–	146	17	303	45	67	52	26
$529 = 23^2$	23.2.11	10	74	350	433	197	113	298	413	5	–	182	420	95	356	53	132
$625 = 5^4$	125.4	2	1	107	–	485	476	139	173	418	431	162	48	329	44	195	97
$729 = 3^6$	243.2	2	1	–	23	394	283	332	33	318	389	199	344	258	215	454	385
$841 = 29^2$	29.4.7	2	1	537	302	376	81	662	469	625	804	–	421	311	203	321	39
$961 = 31^2$	31.2.3.5	3	624	1	440	658	323	401	727	214	87	459	–	835	74	889	366
$N = 2^n$.	$\frac{1}{2}\varphi(N)$.																
$4 = 2^2$	1	–	–	–													
$8 = 2^3$	2	3	–	1	–												
$16 = 2^4$	4	3	–	1	3	2	–										
$32 = 2^5$	8	3	–	1	3	6	7	5	–								
$64 = 2^6$	16	3	–	1	11	14	7	5	4	13	10	9	8	–			
$128 = 2^7$	32	3	–	1	11	14	7	5	20	29	26	9	24	19	10	31	4
$256 = 2^8$	64	3	–	1	11	46	39	5	52	61	26	9	24	19	42	31	36
$512 = 2^9$	128	3	–	1	11	46	39	69	52	125	26	73	88	19	105	31	100

VI. — Décomposition de $2^n \pm 1$.

n.	$2^n - 1$. Diviseurs algébriques.	$2^n - 1$. Diviseurs primitifs.
1		1
3		7
5		31
7		127
9	7	73
11		23.89
13		8191
15	7.31	151
17		131071
19		524287
21	7^2.127	337
23		47.178481
25	31	601.1801
27	7.73	262657
29		233.1103.2089
31		2147483647
33	7.23.89	599479
35	31.127	71.122921
37		223.616318177
39	7.8191	79.121369
41		13367.164511353
43		431.9719.2099863
45	7.31.73.151	631.23311
47		2351.4513.13264529
49	127	4432676798593
51	7.131071	103.2143.11119
53		6361.69431.20394401
55	23.31.89	881.3191.201961
57	7.524287	32377.1212847
59		179951.3203431780337
61		2305843009213693951
63	7^2.73.127.337	92737.649657
65	31.8191	145295143558111
67		193707721.761838257287
69	7.47.178481	10052678938039
71		228479.48544121.212885833
75	7.31.151.601.1801	100801.10567201
81	7.73.262657	2593.71119.97685839
87	7.233.1107.2089	4177.9857737155463
89		618970019642690137449562111
99	7.23.73.89.599479	199.153649.33057806959
105	7^2.31.71.127.151.337.122921	29191.106681.152041
107		162259276829213363391578010288127
117	7.73.79.8191.121369	937.6553.86113.7830118297
127		170141183460469231731687303715884105727

VI. — Décomposition de $2^n \pm 1$ (*suite*).

n.	2^n+1.	
	Diviseurs algébriques.	Diviseurs primitifs.
1.......	3	1
3.......	3^2	1
5.......	3	11
7.......	3	43
9.......	3^3	19
11.......	3	683
13.......	3	2731
15.......	3^2.11	331
17.......	3	43691
19.......	3	174763
21.......	3^2.43	5419
23.......	3	2796203
25.......	3.11	251.4051
27.......	3^4.19	87211
29.......	3	59.3033169
31.......	3	715827883
33.......	3^2.683	67.20857
35.......	3.11.43	281.86171
37.......	3	1777.25781083
39.......	3^2.2731	22366891
41.......	3	83.8831418697
43.......	3	2932031007403
45.......	3^3.11.19.331	18837001
47.......	3	283.165768537521
49.......	3.43	4363953127297
51.......	3^2.43691	307.2857.6529
53.......	3	107.28059810762433
55.......	3.11^2.683	2971.48912491
57.......	3^2.174763	571.160465489
59.......	3	2833.37171.1824726041
61.......	3	768614336404564651
63.......	3^3.19.43.5419	77158673929
65.......	3.11.2731	131.409891.7623851
69.......	3^2.2796203	139.168749965921
75.......	3^2.11.331.251.4051	1133836730401
77.......	3.43.683	617.78233.35532364099
81.......	3^5.19.87211	163.135433.272010961
83.......	3	499.1163.2657.155377.13455809771
87.......	3^2.59.3033169	96076791871613611
91.......	3.43.2731	224771.3126640270656448 1
97.......	3	971.1553.31817.1100876018364883721
99.......	3^3.19.67.683.20857	5347.242099935645987
105.......	3^2.11.43.281.331.5419.86171	211.664441.1564921
111.......	3^2.1777.25781083	3331.17539.107775231312019
135.......	3^4.11.19.331.87211.18837001	811.15121.3858386426478 91

VI. — Décomposition de $2^n \pm 1$ (*suite*).

$$2^{2n}+1 = \left(2^n - 2^{\frac{n+1}{2}} + 1\right)\left(2^n + 2^{\frac{n+1}{2}} + 1\right),\quad n \text{ étant impair.}$$

n.	$2^n - 2^{\frac{n+1}{2}} + 1$. Diviseurs algébriques.	Diviseurs primitifs.
1		1
3	5	1
5	5^2	1
7		113
9	13	37
11	5	397
13	5	1613
15	13.41	61
17		137.953
19	5	229.457
21	5.29	14449
23		277.30269
25	41	101.8101
27	5.109	246241
29	5	107367629
31		5581.384773
33	13.2113	312709
35	5^2.29	4739238 1
37	5	149.184481113
39	13^2.53.157	313.1249
41		181549.12112549
43	5	175921765581
45	5^2.109.1321	181.54001
47		3761.7484047069
49	113	4981857697937
51	5.26317	409.3061.13669
53	5	1801439824104653
55	41.2113	415878438361
57	13.525313	2754153O3169
59	5	1181.3541.157649.174877
61	5	733.1709.368140581013
63	13.37.113.1429	118750098349
65	41.53.157	1081409855868 1
67	5	269.10972041083456992 1
69	5.1013.1657	70334342823809
75	5^3.1321.268501	1201.118246860 1
81	13.37.279073	180121996204 27777
85	5^2.26317	1021.4421.1302647724886 1
87	13.536903681	221702141925004 21
91	5.29.1613	1093^2.886108519077490 9
99	5 109.397.432748	42373.159756072822 73
105	13.41.61.113.1429.741636 1	104181586569018 1
135	13.37.41.61.279073.29247661	541.49681.165041853060421
165	5^2.397.1321.4327489.363010552014 1	661.3301.8581.1212762735030 1

VI. — Décomposition de $2^n \pm 1$ (*suite*).

$$2^{2n}+1 = \left(2^n - 2^{\frac{n+1}{2}} + 1\right)\left(2^n + 2^{\frac{n+1}{2}} + 1\right), \quad n \text{ étant impair.}$$

n.	$2^n + 2^{\frac{n+1}{2}} + 1$.	
	Diviseurs algébriques.	Diviseurs primitifs.
1		5
3		13
5		41
7	5	29
9	5	109
11		2113
13		53.157
15	5^2	1321
17	5	26317
19		525313
21	13.113	1429
23	5	1013.1657
25	5^3	268501
27	13.37	279073
29		536903681
31	5	8681.49477
33	5.397	4327489
35	41.113	7416361
37		593.231769777
39	5.1613	3121.21841
41	5	10169.43249589
43		173.101653.500177
45	13.37.41.61	29247661
47	5	140737471578113
49	5.29	197.19707683773
51	13.137.953	1326700741
53		15358129.586477649
55	5^2.397	363010552014 1
57	5.229.457	131101.160969
59		5764607533771653 13
61		3456749.667055378149
63	5.29.109.14449	40388473189
65	5^2.1613	521.51481.34110701
69	13.277.30269	54156240237 49
73	5	293.9929.649301712182209
75	13.41.61.101.8101	63901.13334701
77	113.2113	8317.76096559910757
81	5.109.246241	1801659766697 1649
87	5.107567629	349.29581.27920307689
93	13.5581.384773	373.951088215727633
99	13.37.2113.312709	235621.8463901912489
105	5^2.29.1321.14449.4739238 1	421.146919792181
129	5.1759217765581	17029.46957.9675877154368 6753
135	5^2.109.181.1321.54001.246241	30241.166242935471754241

VI. — Décomposition de $2^n \pm 1$ (*suite*).

$2^{4n}+1$.

$4n$.	Diviseurs algébriques.	Diviseurs primitifs.
0		1
4		17
8		257
12	17	241
16		65537
20	17	61681
24	257	97.673
28	17	15790321
32		641.6700417
36	17.241	433.38737
40	257	4278255361
44	17	353.2931542417
48	65537	193.22253377
52	17	858001.308761441
56	257	5153.54410972897
60	17.241.61681	4562284561
64		274177.67280421310721
72	97.257.673	577.487824887233
76	17	1217.148961.24517014940753
80	65537	414721.44479210368001
84	17.241.15790321	3361.88959882481

INDEX ALPHABÉTIQUE

Les numéros inscrits sont ceux des pages correspondantes.
Les noms d'auteurs sont imprimés en *italique*.

ERRATA.

Plusieurs erreurs typographiques se sont malheureusement glissées au cours de l'impression de cet Ouvrage. Nous donnons ci-dessous les principales. Le lecteur corrigera facilement de lui-même les autres.

Pages.	Ligne [1].	*Au lieu de :*	*Lire :*
9	— 10	22	2^2
13	— 8	premiers avec	inférieurs à N
36	— 3	3	— 3
38	12	2	— 2
40	— 8	12	— 12
39	— 1	$x \equiv 3 \pmod{4}$	$x \equiv 2 \pmod{4}$
40	7	$x \equiv 586$	$x \equiv 386$
47	6	les deux termes	les termes
51	3	$2^n - 1$	$a^n - 1$
60	— 4	$z^2 - p$	$z^2 - z$
61	6	$\equiv 0$	$\equiv 1$
67	9	supérieurs	inférieurs
76	7	il vient	il vient à un multiple de p près
83	17	$x^2 \equiv \pm b$	$x \equiv \pm b$
117	8	a^m	am
120	9 et 11	7313, 5353	7613, 6353
139	17	3706	3607
193	— 8	$N \equiv 9.\ 2.3.4.7$	2.4.6.7

128 Les nombres 3 et 9 du tableau doivent être permutés.

121-122 Les indices suivants doivent être corrigés :

N =	11	19	29	31	41	47	59	61	67	73	79	83
Ind N =	7881	6418	1399	6218	6739	3622	8243	4655	8116	6823	6922	6916

(1) Le trait placé devant un chiffre signifie que les lignes sont prises en remontant.

TABLE DES MATIÈRES

CHAPITRE III. — *Généralités sur les congruences de degrés supérieurs.*

CHAPITRE IV. — *Congruences du second degré.*

Chapitre V. — *Congruences binomes, Indices. Congruences exponentielles.*

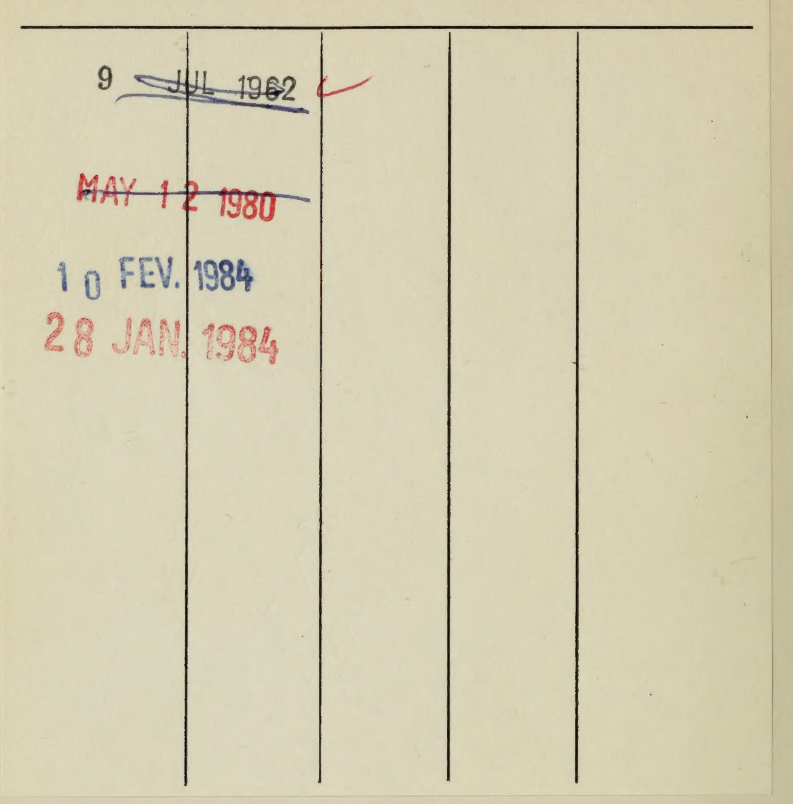
Chapitre VI. — *Factorisation.*

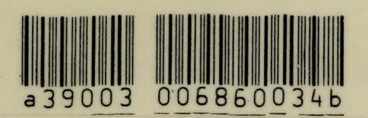
TABLES.

FIN DE LA TABLE DES MATIÈRES.



PARIS. — IMPRIMERIE GAUTHIER-VILLARS ET Cie,
Quai des Grands-Augustins, 55.
66178-22


9 JUL 1962
MAY 12 1980
10 FEV. 1984
28 JAN. 1984


a39003 006860034b